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

Noellie Brockdorff, Christine Garzia
Department of Cognitive Science, University of Malta, Msida, Malta

May 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 Malta results of a qualitative study undertaken as part of the SMART project – "Scalable Measures for Automated Recognition Technologies" (SMART; G.A. 261727). The analysis and results are based on a set of 3 focus group discussions comprising of 28 participants from different age groups, which were held in order to examine the awareness, understanding, beliefs and attitudes of citizens towards smart surveillance and privacy.

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

The Maltese participants were highly aware of being under surveillance in different contexts including commercial, boundary and public spaces. Participants mentioned a wide range of surveillance technologies and methods, including the use of loyalty cards with the aim of monitoring consumer behaviour and the use of CCTV systems in order to observe citizens in various spaces. Overall, surveillance directed at consumers was perceived as taking place mainly for security, marketing and advertising purposes, while general citizen surveillance was regarded as occurring for reasons of national security and personal safety. Most participants were also aware of the extent of surveillance when using a mobile device, which they perceived as occurring for commercial and security reasons.

In order to gauge participants' attitudes and beliefs on massively integrated dataveillance, a fictional scenario illustrating the massive integration of data was presented to participants. After an initial intense reaction, the possibility of integrated dataveillance actually occurring was discussed from a technical, legal and ethical perspective. In general, participants considered the massive integration of personal data as currently possible from a technical point of view, although not to the extent portrayed in the scenario. Notwithstanding this belief, most participants questioned the occurrence of dataveillance since they perceived this practice not only as illegal but also as unethical. Moreover, in all focus groups, participants expressed a strong belief that the likelihood of massively integrated dataveillance taking place would also depend, in part, on citizens' self-responsibility in divulging their data, especially in the context of virtual spaces. In addition to the likelihood of massively integrated dataveillance, participants also discussed its acceptability. Ethical considerations were raised by most participants, who perceived integrated dataveillance as unacceptable primarily due to privacy reasons. Participants also drew attention to a number of perceived risks, mainly in relation to data misuse and misappropriation. Nevertheless, participants also mentioned that dataveillance could serve as a valuable tool for law enforcement purposes and for the enhancement of citizen and customer services. Overall it appears that acceptance was contingent on several factors, including purpose of use, giving consent, type of data, as well as which entity – state or private – would have access to the data.

The effectiveness of smart technologies was also discussed, with smart surveillance understood as being capable of autonomous decision-making. While some regarded automated systems as more efficient in comparison to those requiring a human operator, others appeared to be sceptical of technology on its own without human agency. Overall, it seems that several participants preferred a combination of technologically-mediated surveillance and human operators in the surveillance process. Moreover, participants also discussed the perceived privacy impact of smart technologies. Once again opinions varied and while some objected to being surveilled irrespective of whether surveillance technologies are fully automated or not, others argued that whether the system is fully automated or not is irrelevant since the information is available in both cases. In contrast, some participants appeared to prefer automated systems since they considered such systems as having less of a negative impact on privacy.

The intensification of surveillance was perceived as posing a threat not only to privacy but also to freedom. Participants associated a number of risks with intrusive surveillance, including the risk of misuse and misappropriation of surveillance data. On the other hand, a minority of participants appeared reassured with the presence of surveillance measures and expressed their willingness to sacrifice their privacy for increased security. Overall the majority of participants showed a rather critical and questioning attitude towards the use of surveillance and generally appeared unwilling to sacrifice their privacy even in case of an increase in the level of threat. With regards to views on the different types of surveillance technologies, some general patterns could be noted. With some exceptions, video-surveillance in public places was generally acceptable, while views on the use of biometric data were polarised. In contrast, most regarded the electronic tagging of vulnerable populations as extremely controversial, with only a minority of participants considering the use of this method as acceptable.

Participants also shared their viewpoints on current surveillance laws and regulations. The predominant sentiment appears to indicate that the participants do not feel sufficiently protected by the Data Protection Act. Two major problems highlighted by most participants were the lack of enforcement by the authorities and the existence of loopholes in the legislation. Overall it appears that the participants have a low level of trust in the Maltese judicial system. In relation to the length of storage of surveillance data, expectations were varied; while some suggested different time-frames ranging from one week to six months, others suggested longer periods, including an indefinite period, for any possible future use.

2. Introduction

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

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

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

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

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

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

3. Methodology

In total, 42 focus groups – three in each country – were conducted between February and November, 2013. Thirty-nine of the groups had between 6 and 10 participants, three groups had 11, 12 and 13 participants respectively. Overall, 353 participants took part in this research project. The focus groups in Malta were carried out on the 3rd, April, 2013; 5th April, 2013 and 9th April, 2013. The composition of the groups held in Malta 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 Maltese version of the discussion guidelines can be found in Appendix C.

3.3 Focus group procedure

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

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

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

3.4 Data analysis

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

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

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

4. Description of the Sample

The data analysis for Malta is based on a total of 28 participants, out of which 12 were males and 16 were females. Group 1 (18-24 years) was in the main composed of students and graduates from different fields of study. Group 2 (25-44 years) was composed of workers from different occupational backgrounds although more than half of the participants held jobs in the education sector and in the social sciences field. Lastly, Group 3 (45+ years) was composed of workers from different occupational backgrounds, one houseperson and two retirees.

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	M	M
P2	M	M	M
P3	M	M	M
P4	M	M	F
P5	M	F	F
P6	F	F	F
P7	F	F	F
P8	F	F	F
P9	F	F	-
P10	F	F	-
Total	**10**	**10**	**8**

In general the atmosphere of the three groups was friendly and informal, and the overall flow of the discussion was smooth in all three groups. Most of the participants were rather enthusiastic and engaged well with the topic under discussion, and several participants willingly recounted and shared personal experiences related to surveillance. At times the discussion was rather heated and animated, but the participants still listened to and respected each other's viewpoints.

While in Group 2 all participants contributed to the discussion and there was no one who was considered as particularly dominant or reserved, in the other two groups some participants stood out. In particular, one participant in Group 1 (P1) proved to be rather talkative and at times tended to dominate the discussion, although not in a forceful manner. This participant was particularly keen on sharing his opinions which might to a certain extent be attributed to his academic background in Computer Engineering and thus to his keen interest in technology. On the other hand, the input of two participants from Group 1 (P3 and P10) and three participants from Group 3 (P6, P7 and P8) was rather limited and it proved difficult to get them involved in the discussion.

5. Results

5.1 Surveillance Technologies in Different Spaces

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

5.1.1 Commercial Space

Participants in all groups were aware of being under surveillance in a commercial context and the predominant methods mentioned through which consumers are surveilled were video-surveillance systems, the use of loyalty cards and the monitoring of financial transactions by banks. Moreover, the possible monitoring of customers by staff and security personnel was also mentioned by some of the participants.

The use of loyalty cards was perceived as having several purposes, mainly relating to the monitoring of consumer patterns for marketing and advertising purposes: "*Well, every time you use a loyalty card they can see what you're buying and so they can add to their database all the items you buy, every time. And so then they can send you offers and things like that"* (P8-I). In addition to contributing to advertising and marketing, consumer data was also perceived as a valuable tool in helping the commercial establishment strategically arrange store and shelf layouts: *"[…] they will know what products to place where"* (P1-I); this was perceived by the participants as a tactic to increase turnover. A number of participants argued that the attractive incentives linked to the use of loyalty cards, such as providing special offers to customers, in practice served these rather covert purposes: *"They keep track of what you buy, with the pretext that you're collecting points […]"* (P8-II). In general, customer data was perceived as a highly profitable *"commodity"* (P1-III) due to the belief that in addition to being used by the commercial establishment collecting it, it could also be sold to third parties, including companies involved in market research.

Participants regarded video-surveillance systems as being in place solely for security purposes; the investigation of crime was mentioned as a primary purpose in this context: *"I think they're just there as a safety feature – just in case something gets stolen and then they can refer to it"* (P1-I). It appears that while some of the participants believed that security personnel monitor the CCTV screens in real time, others argued that unless an incident happens, *"nobody"* (P1-I) watches the recordings: *"I very much doubt that they bother to watch them"* (P10-II). While some expressed their annoyance at the use of video-surveillance in commercial establishments, *"I'm used to it but I'm not really very happy with it"* (P10-II), others appeared indifferent: *"If you're not doing anything wrong why bother? […] It doesn't really bother me"* (P1-II). On the other hand, others seemed to appreciate the presence of video-

surveillance in this context: *"Cameras make you feel safe […] it's not the first time you see things like hold-ups and you say to yourself 'If I had been there what would have happened?'"* (P2-II).

Lastly, a number of participants also mentioned the monitoring of financial transactions by the banks: *"[…] the credit card you use to pay for things is also a record of how often you go to the supermarket, how much you are spending, where you are going shopping"* (P5-II). Overall it appears that the participants were aware of being under surveillance through different means in a commercial context and on the whole, most participants considered the monitoring of consumers in these ways as justified.

5.1.2 Boundary Space

In the context of border control, the discussion mainly focused on an airport setting as a boundary space. Surveillance in airports was perceived as ubiquitous: *"They are watching everything […] they are dissecting [you]"* (P1-II) and as extremely thorough: *"They would know practically everything about you"* (P1-I). The primary purposes of surveillance in this context were perceived as being national security and passenger safety, while to a lesser extent a minority of participants mentioned commercial motivations.

At the outset, some participants argued that surveillance in the context of air travel starts *"when you buy the ticket"* (P4-III). A range of monitoring methods and surveillance technologies in use in airports was mentioned by the participants in all groups. The use of video-surveillance was considered as being widespread in this context and, as well as the use of traditional CCTV mentioned by several participants, one participant also mentioned the use of smart CCTV: *"They capture certain behavioural movements on CCTV cameras"* (P1-I). In addition to the use of biometric passports, the use of smart surveillance in this context was also alluded at, albeit at times in an unsure manner as to the exact nature of such technologies: *"And there are places where they even put you in front of some eye machine […]"* (P9-II). Other frequently mentioned methods of surveillance included different object and product detection devices, such as luggage controls and body scanners. The monitoring of personal data via the airline booking system, the flight manifest, and passport control was also discussed. Some participants also mentioned surveillance by airport security staff including *"guards holding machine guns"* (P1-II), plain clothes police officers and also the use of sniffer dogs. Overall it appears that participants were generally intensely aware of being surveilled by a variety of entities including airport security services, commercial entities such as airline companies, government authorities, foreign governments and international agencies such as Interpol.

National security and passenger safety were perceived as the primary purposes of surveillance at airports. In particular, participants mentioned a preventive function by the prior identification of individuals *"who pose a risk"* (P4-I); this was especially the case where *"terrorist acts"* (P5-II) were concerned. Others additionally mentioned that surveillance data could be employed for investigation purposes, thus serving as evidence *"in case something happens"* (P2-II). While some participants accepted surveillance at airports as *"an obvious process"* (P4-II) contributing to passenger safety: "*No it*

doesn't bother me since it makes me safe to travel […] the more security that there is, the better" (P2-II), several others expressed their discomfort at being scrutinised so thoroughly: *"It seems as if they are always treating you as guilty you know? I don't like it*" (P6-II). Also mentioned, but to a lesser extent, by some participants was that the collection of data and statistics in the context of air travel additionally satisfies various commercial motivations and functions by different private and state entities including airports, airlines, travel agencies as well as tourism authorities:

> *"I think this has many facets: there's security for one thing […] and then there's the commercial side, which is important too. It starts with the internet when you book your seat online, or when you go to a travel agent, since they have every interest in knowing who uses their services. The airlines as such need to know, as well as the tourist boards. In fact the local airport has very often conducted surveys about tourists entering the country as such. Then again they want to know for commercial reasons. This sort of information is very important to them" (P1-III).*

Lastly, some participants argued that the extent of surveillance at airports is dependent, in part, *"on where you're travelling"* (P5-I). Several participants pointed out that at certain airports, security measures can be "*stricter"* (P9-I) and *"more invasive"* (P4-III). To emphasise this point, several participants made comparisons between different countries:

> *"It depends where you pass from. You know, let me mention Israel again, not only do they check [your travelling documents], but they delve into your family and history, [family] roots and all. So it depends on where you're travelling. If you're passing through Italy and through Malta, no one really bothers that much! But if you're passing through Switzerland, they will check you and take you in a room […]" (P5-I).*

5.1.3 Common Public Spaces

In common public spaces, such as stadiums where mass events like sports matches and concerts are organised, participants mentioned a range of methods through which surveillance occurs. All focus groups mentioned the use of CCTV as a primary means of surveillance in this context and, additionally, some participants also drew attention to the possibility of being inadvertently recorded by any television cameras filming the event. The monitoring of personal data via the purchase of tickets as well as the use of metal detectors and security checks upon entrance to the event was also mentioned: *"They check the things you're bringing in with you, your bag and its contents"* (P6-I). Moreover, one of the participants from Group 2 (25-44 years) also mentioned audio surveillance with the aim of monitoring hate speech: *"There would be lots of security personnel in a control room, watching the video, recording [what people are saying] and they fine whoever passes racist remarks"* (P9-II). In addition to technological surveillance, all groups also mentioned the presence of security officers and law enforcement personnel.

In general, the predominant function of surveillance in public places was perceived as being public security and citizen safety. It appears that surveillance in this context was perceived as justified by the

majority of participants, as long as the necessary steps are taken to inform the public that monitoring is taking place:

> *"At the end of the day you are in a public place. If you are in a public place it's not your home. I believe that since you are in a public place, you are prone to these things [being monitored]. What I don't agree to is when perhaps you are not informed about it. You should be told beforehand" (P2-II).*

5.1.4 Mobile Devices and Virtual Spaces

The majority of participants in each of the groups appeared to be aware of the extent of surveillance when making use of a mobile device: *"[…] you are leaving a trail behind, everywhere you go, everywhere you browse"* (P4-III). Participants discussed a range of methods through which technologically-mediated surveillance occurs, or can potentially occur, within this context. The most frequently mentioned methods were location tracking through GPS, as well as the monitoring of call lists and message lists, which was perceived as occurring for commercial reasons: *"The service provider would know the exact location, how often you're phoning, whom you're calling, at what time, how long your call took, [a log of] your messages. Everything can be known. Everything, absolutely everything!"* (P1-I). In particular, location data was regarded as extremely sensitive and location tracking was perceived as presenting possible risks, such as burglaries while home owners are on holiday:

> *"Location data is sensitive because if I go abroad, I would be letting everyone know that I'm not home for a week […] if there are people, hackers, who are able to enter the systems [of service providers], they are quite capable of finding the information because it's there, whether you want it or not" (P1-I).*

Moreover, specifically in relation to smartphones, some participants expressed concern at the possible risks involved in being connected to the internet through mobile devices:

> *"They [my family] bought me a mobile phone with internet capability, and I don't want it! I told them to remove the internet because I try to use it the bare minimum possible […] somehow having internet on it I feel even more exposed. I don't like it" (P5-III).*

Significantly fewer participants, mostly from Group 1 (18-24 years), mentioned the collection of data through the use of smart phone applications; here one participant argued that most users are very naïve in this regard and especially unaware of possible risks: *"You download an app, press 'sign' and 'accept', [you] always press 'accept', 'accept', 'accept', and you don't see what's happening […]"* (P1-I). Several participants from this group agreed that individuals tend to divulge their personal data *"without thinking that it might fall into the wrong hands"* (P6-I).

When asked about how they felt about being monitored in such ways, the reactions of the participants were rather mixed, with some admitting that surveillance is akin to *"a two-edged sword"*: *"It's got a*

good side and it's got a bad one. It depends on how it's used" (P6-I). While several participants pointed out the detrimental effect of mobile phone usage on privacy: *"Your privacy is compromised […] your privacy is completely gone, my belief is that it's gone, one hundred percent [gone]"* (P2-III), others were quick to emphasise that in certain situations, this type of monitoring could prove beneficial. In particular, the latter participants mentioned that location tracking could be useful to citizens in cases ranging from theft: *"[…] for instance if they steal your mobile they can trace it"* (P6-I) to emergency situations: *"It could be a life saver as well in certain cases"* (P6-II). Moreover, from a law enforcement perspective, others additionally mentioned the utility of this type of monitoring for the investigation and prosecution of criminal cases: *"[…] some [court] cases are being decided on [the basis of] a telephone call"* (P6-III).

5.2 Perceptions & Attitudes towards Smart Surveillance and Integrated Dataveillance

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

5.2.1 Feelings

After having listened to this conversation, the focus group participants revealed different feelings, predominantly including an extreme sense of disbelief, feelings of discomfort and anger. Firstly, some participants found it difficult to conceptualise that this *"outrageous"* (P1-II) scenario could actually occur: "*Oh this is nonsense, it can't happen"* (P4-II). In line with this, a number of participants stated they would feel *"shocked"* (P6-I) and *"dumbstruck"* (P2-I) should they experience this first-hand. Additionally, feelings of discomfort were common in all three groups, with participants expressing that in such circumstances they would feel *"exposed"* (P9-I), *"suffocated"* (P3-II), "*unnerved*" (P10-II) and *"breathless"* (P4-III). Lastly, several participants perceived this as a *"huge invasion"* (P6-II) and expressed feelings of frustration and anger. These participants stated they would feel *"very annoyed"* (P7-III) and *"mad"* (P5-I) at such *"inappropriate behaviour"* (P7-I) by a civil servant: *"I think I would have started insulting her! I would start insulting her that very moment!"* (P8-II)

5.2.2 Behavioural Intentions

In addition to asking about their feelings upon listening to this conversation, participants were also asked for their resulting behavioural intentions. In line with the belief that such an occurrence would not only be totally unacceptable but also illegal, several participants claimed they would resort to different legal measures. Firstly, one of the actions mentioned was investigating the legitimacy of the situation: *"I would phone my lawyer to see if they had any right to do that, to check my rights […] if I could I would record the conversation there and then, so that I would have proof"* (P10-II). Additionally, others stated they would either report the incident to the Data Protection Commissioner or else file a police report: *"I would go straight to the police"* (P9-I). On the other hand, some of the participants preferred taking matters into their own hands and stated they would confront the civil servant there and then: *"I would ask her 'How do you know this information?'"* (P9-II), and proceed to investigate.

[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.

In contrast to the above reactions, others suggested a rather passive reaction involving some kind of immediate withdrawal from the hypothetical situation, which primarily included hanging up the phone: "*I would have stopped talking to her straightaway. I'm sure"* (P6-II). Similarly, another participant from the same group stated: *"I don't know if I would have continued with the conversation"* (P5-II). Additionally, perhaps reflecting his feelings of disbelief, one of the participants stated *"I would leave this country if that happened!"* (P2-III).

5.2.3 Beliefs

5.2.3.1 Likelihood of smart surveillance and integrated dataveillance

Regarding the likelihood of whether or not smart surveillance and massively integrated dataveillance are possible (currently or in the future), the focus group participants distinguished between technical, ethical and legal aspects. Generally, while the first reactions were of shock and disbelief, after reflecting on this hypothetical situation the majority of participants deemed the development of massively integrated dataveillance as certainly possible from a technical aspect, albeit not to the extent as portrayed in the scenario, which was considered by most as "*an exaggeration"* (P4-III). The majority of participants perceived the scenario as being *"all too possible"* (P1-I), a belief which appeared to stem from the assumption that it is feasible to integrate data on a massive scale given that it is already available, albeit it is currently *"very scattered"* (P1-III). Therefore, from a technical perspective, most participants argued that it is only a matter of time before such systems are developed and introduced: "*It's not very far away in the future. It is [technically] possible now if they want to"* (P4-III).

Nevertheless, although technically feasible, the majority of participants from all the groups questioned the likelihood of massively integrated dataveillance from a legal perspective. In line with the strong reactions outlined earlier, most participants considered the hypothetical case as illegal: *"It is not permissible"* (P4-I). Moreover, ethical considerations were brought up by the participants who perceived the massive integration of data as *"unacceptable"* (P1-I) and *"unethical"* (P9-I) primarily due to privacy reasons: *"They know everything about you! I don't know what else they could tell you about yourself!"* (P6-II). Nevertheless, some participants appeared resigned that such practices cannot be halted and conveyed concern that *"the world is changing"* (P5-I) in this direction.

In all focus groups, several participants expressed a strong belief that the likelihood of massively integrated dataveillance taking place would depend to a certain extent on individuals' self-responsibility in divulging their personal information: *"We have to take responsibility"* (P2-III). Several participants claimed that individuals tend to be *"naïve"* and *"give out [their] data rather freely"* (P10-II), since they do not realise *"the potential risk that they're putting themselves in"* (P3-III). Thus they proceeded to argue that citizens should be more aware of the impact of their behaviour in this regard: *"And sometimes we are the ones giving this information away! We are exposing ourselves […] very often it's our fault"* (P5-I). The discussion here also revolved around self-responsibility in the context of virtual

spaces and in this regard, it appears that a main concern by some of the participants was the permanency of data traces: *"Most do not realise that the internet, as far as we know, is going to leave a trail forever"* (P4-III). More specifically, some participants appeared to immediately make sense of the scenario by linking it to the use of online media such as social networks:

> *"In reality one can easily get hold of this information […] If you post on Facebook, I don't know, "Today I am going out with Elisa for a coffee, see you", everybody, some 400 friends [would read the post], some would press like, just imagine how many people would know" (P5-I)*

5.2.3.2 Acceptance of smart surveillance and integrated dataveillance

After discussing the likelihood of massively integrated dataveillance, the participants also discussed its acceptability. As mentioned previously, an overwhelming majority of participants regarded the scenario as clearly unacceptable since they perceived it as a *"huge invasion"* (P6-II): *"In that scenario I would say there's no privacy"* (P3-III). In relation to this, some participants agreed that technology has a negative impact on privacy and that technological advancements have resulted in a situation where *"our personal life doesn't exist any longer"* (P6-II). At the same time, however, the same participants argued that surveillance is, to a certain extent, undergoing a process of normalisation: *"It's normal. It's happening every day. These are things that we have sort of ended up accepting"* (P6-II). In this regard, some participants from Group 1 (18-24 years) and Group 3 (45+ years) perceived the normalisation of surveillance as a *"generation thing"* (P8-I), with some suggesting that young adults tend to have a nonchalant attitude towards the sharing of personal data:

> *"We [young people] were born into it and for instance you take out your loyalty card, give your ID card number every day, but my mother takes ages checking and reading the application form. I fill it up straight away. I don't even pay attention […] I mean we have gotten so used to this sort of thing, we don't even realise how unsafe it is" (P8-I).*

Overall it appears that participants' acceptance of massively integrated dataveillance depended on a number of factors, including purpose of use, whether consent was expressly provided and type of data to be collected and shared. Another matter which had a bearing on the acceptance of dataveillance was the issue of which entity, state or private, would have access to such data. Firstly, some participants discussed purpose of use, which was considered as a major factor influencing acceptability to dataveillance:

> *"Certain things, before you implement them and set them up, you need to see them in their context, how they are going to be used, and you should take enough precautions and keep on using them only for that particular use […] we need to be careful that the technology is going to be used up to a certain limit" (P6-I).*

In this regard, participants mentioned specific uses in circumstances which they considered as acceptable, including cases where dataveillance was regarded as a valuable tool for the prevention and investigation of crime such as fraud. Dataveillance was also perceived by some participants as acceptable in cases where it enhanced service efficiency and was thus considered as facilitating user convenience: "*On the other hand I like it because it makes life easier. Because if you go somewhere, anywhere and everybody has the information, that's convenient, isn't it?* (P1-I). However, notwithstanding these perceived advantages, most participants were very keen to point out a number of risks mainly in relation to data misuse. First of all, some pointed out that data could potentially be manipulated "*for wrongful purposes"* (P1-I) by those persons who are authorised and entrusted with access to citizen data. All that amount of information accessible to one person was perceived as extremely risky and as creating a power imbalance between citizens and surveillants:

> *"What bothers me is that there is one person who knows everything about me. That bothers me because I don't know who she is […] there will always be abuse [of the information]. If there is somebody who, I don't know, has taken an oath of office and holds a certain position sort of, but even then, you can't trust that person. That's why it bothers me […]" (P1-II).*

Linked systems were also perceived as substantially increasing risks of misappropriation: *"[…] and the more they become connected, the greater will be the possibility of information leaking out"* (P3-III). In fact, another major concern was data theft, which was considered by some participants as a very real threat: *"What if someone were to steal the data? This makes me feel very exposed […] someone, third parties, could abuse the system, or else it could be stolen"* (P10-II). More specifically, some participants mentioned the possible risks of identity theft or identity fraud:

> *"What worries me most is that there could be someone who is really savvy, who would use your IP address to do something illegal using your identity. That's my biggest worry and that is so easy to do […] Just try to go and prove it wasn't you!" (P4-III).*

Another factor influencing the participants' acceptance of dataveillance was whether consent was given by the individual whose data was being shared. Some participants argued that unless permission is expressly given, the sharing of personal information would be deemed as unacceptable. In fact it seems that one of the major reasons why the hypothetical scenario resulted in feelings of anger was the lack of consent: *"In this case it was done behind his back, you see? That's what is so bad about it"* (P6-I). In addition to the issue of consent, a further aspect which had a bearing on the acceptance of dataveillance was the type of data to be shared. Overall, participants agreed that the most confidential data included location, financial information, sexual orientation as well as medical and health data, all of which were regarded as *"too personal"* (P9-II). With regards to the risks of data sharing, it appears that one major concern amongst some of the participants in Group 1 (18-24 years) was that the sharing of sensitive data could in certain cases result in discrimination, especially in an employment-related context.

Participants also discussed data sharing by the state and by commercial enterprises. In general, it appears that attitudes with regards to data sharing by the state were mixed. Some participants adamantly agreed that information between government departments should not be shared: *"I don't agree that data should be shared between one department and another, because one is in no way relevant to the other"* (P1-I). In case data was to be shared, participants argued that this should not happen in an underhanded manner: *"They shouldn't just go on with that [data sharing] without my knowledge, I want to be aware that different departments are pooling information about me"* (P9-I). On the other hand, others argued that data sharing between government entities should be possible *"on a need to know basis"*:

> *"For instance if I am going to avail myself of a government service, let's say I arrive at the hospital due to an emergency. They shouldn't need to know my revenue, they shouldn't need to know whether I go to school or not - but if it's a service that normally comes at a price but is waived for students then it's understandable. But [then] there should be strong safeguards in place" (P2-I).*

While attitudes towards data sharing by the state were noticeably mixed, data sharing between commercial entities was generally considered by most participants as *"unethical"* (P4-III) and *"very annoying"* (P5-I) in cases where consent was not expressly provided by the individual. In relation to this it appears that data sharing between private entities *without consent* was considered by some participants as a rampant practice: *"It's very much in existence"* (P2-I). Notwithstanding the mostly negative reaction towards data sharing in a commercial context, a minority of participants did argue that this practice could sometimes result in certain advantages for the consumer: *"But as regards commercial ones, however, there is also a good side to it. If someone rings you up for commercial reasons and they let you know about a good offer, you won't be annoyed to hear them out"* (P6-I).

On a last note, since the focus groups in Malta were held a few weeks after a general election, participants in all three groups shared their experiences of rampant data sharing of contact details such as mobile phone numbers and e-mail addresses by political parties during their respective electoral campaigns:

> *"During the run up to the election I received messages from people in parliament or electoral candidates whom I don't know personally and have no idea how they got hold of my number. [This bothered me] very much! And I still get messages you know, 'thank you for your support', and I don't even know who he is! And I didn't vote for him! In my opinion this is a serious breach of the Data Protection Act. And you cannot even reply!" (P3-II).*

Similarly, a number of participants expressed frustration and some even anger at what they perceived was a blatant and an unlawful sharing of personal data: *"That's supposed to be protected information; it shouldn't have ended up being used for propaganda purposes [by electoral candidates]. And that angered me a lot!"* (P4-III).

5.2.3.3 Perceived effectiveness and privacy impact of smart technologies

Participants from Group 1 (18-24 years) had the most to say about the automatic decision-making process of smart technologies. It appears that the issue of automation produces mixed feelings and beliefs amongst the participants. Firstly, the participants differentiated between decisions taken by humans and those taken by automated technologies. In this regard, some participants argued that humans, unlike machines, introduce an element of subjectivity due to their feelings and judgements: *"The machine isn't biased but a person could be biased"* (P5-I). These participants appeared to believe that technology is much more reliable without human agency: *"I consider technological systems as very safe, when things go wrong it's [because of] the human element"* (P1-I). On the other hand, others appeared to be sceptical and distrustful of technology on its own without human agency: *"A machine doesn't reason"* (P7-I). It was pointed out that one of the downsides of wholly automated systems is that there can be no negotiation or bargaining once a decision is taken by the machine: *"[…] but a person is better because at the end of the day [the decision of] a machine is either a one or a zero"* (P4-I). Nevertheless, in spite of these various beliefs, it appears that the majority of participants agreed that the final decision should ultimately rest with a human operator: *"I think that first there should be a decision by the machine and then you would have a decision from a real person"* (P8-I). The presence of a human operator in the technologically-mediated surveillance process was regarded as providing a number of benefits, including the possibility to *"double check"* (P1-I) a situation, and, as a result, to lessen the risks of *"a false alarm"* (P1-I).

The issue of the privacy impact of surveillance came up during the discussion with participants from Group 2 (25-44 years) and Group 3 (45+ years). Firstly, some participants appeared to express a preference for automated systems since they perceived such systems as having less of a negative impact on privacy: *"If it's an automated system I would worry less [about being observed]"* (P8-II). On the other hand, other participants, mainly from Group 3 (45+ years) adamantly objected to being monitored by surveillance technologies, irrespective of whether they are fully automated or require the intervention of a human operator: *"No for me it's not acceptable either way"* (P5-III). Lastly, others argued that whether the system is fully automated or not is irrelevant since the information is available in both cases: *"In any case, it doesn't make a difference whether it's automatic or not. Once the data is stored it's accessible"* (P2-III).

5.3 Security-Privacy Trade-offs

5.3.1 Acceptance of Technological Surveillance

In order to gauge participants' perceptions vis-à-vis the security-privacy trade-off, as well as their attitudes towards a number of specific smart technologies, a hypothetical scenario was presented to participants. In brief, this scenario depicted the introduction of a number of smart technologies including smart CCTV, automated number plate recognition (ANPR), sound sensors, the collection of various biometric data (fingerprinting, iris scanning and DNA sample) and electronic tagging of vulnerable populations (children and older citizens). The scenario and two variations of the scenario depicted how these surveillance technologies were introduced by the state following different levels of threat experienced by the citizens[4].

When discussing the scenario, the majority of participants from Group 1 (18-24 years) and Group 3 (45+ years) and some participants from Group 2 (25-44 years) had a very intense reaction, perceiving the use of all the aforementioned surveillance measures in conjunction as a *"nightmare"* (P1-III). Participants from the different age groups argued that with the introduction of intensive surveillance, a democratic state could easily develop into a *"dictatorship"* (P10-II): *"We're talking about a police state. God forbid we ever get to this state*" (P2-III). In fact, rather than enhancing feelings of personal safety, the security measures portrayed in the scenario resulted in feelings of discomfort and insecurity amongst most of the participants: *"I'd feel very unsafe"* (P10-II). In this regard, some participants argued that the visibility of certain surveillance measures, in particular overt measures such as cameras, heightens peoples' awareness of the possibility of danger:

> *"When you see a lot of security around, very often this scares you even more. You're more afraid, because they are alarming you […] so I think that security needs to be on a very low key level. It has to be there but it has to be truly low key and not alarming because if it's alarming, people will feel even more scared" (P1-III).*

Nevertheless, in contrast to the predominant sentiment, the views of the participants in Group 2 (25-44 years) were rather polarised; while some participants expressed feelings of insecurity in line with the majority of the participants in the other two groups, several others from this group stated that the surveillance measures depicted in the scenario would enhance their feelings of safety: "*Everything helps to make you feel safe in that environment*" (P8-II) and perceived the introduction of such measures as justified and as completely acceptable: *"I'd feel safe, the more [surveillance measures] the merrier I think. I agree with having it for safety reasons […] I find no objection"* (P2-II). These participants appeared to feel reassured with the presence of surveillance measures and expressed their willingness to sacrifice their privacy for increased surveillance following an increase in crime. One of the participants

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

from this group even expressed his agreement with the introduction of such surveillance measures even in times of relative safety. As noted earlier, these views contrasted sharply with the opinions put forward by the participants in Group 1 (18-24 years) and Group 3 (45+ years), as well as with the rest of the participants in Group 2 (25-44 years), who, upon reflection, showed a rather critical and questioning attitude towards the use of surveillance and generally appeared unwilling to sacrifice their privacy for increased surveillance even in case of an increase in the level of threat.

A number of reasons can be attributed to this increased sense of insecurity and vulnerability amongst the participants. Firstly, several participants expressed concern at the way that surveillance measures affected their privacy, perceiving surveillance technologies as providing a means through which one is constantly being monitored: *"Alright, you may not be doing anything wrong but the fact that there's somebody always watching you, knowing what you're doing, what you're buying, where you're going […]*" (P7-I). Whilst the participants perceived such a situation as severely impinging on their privacy, it appears the use of surveillance revealed even more intense concerns relating to 'freedom', which was considered as *"a fundamental human right"* (P1-I) by the participants. During the discussion, the frustration at the citizens' lack of choice over the government's decision to intensify surveillance was evident: *"Because we are saying that this gives us no choice. This is being enforced by the government, irrespective of whether I want it or not"* (P5-II). Additionally, participants argued that should citizens willingly accept the intensification of surveillance without challenging the introduction of these measures, there would be a risk of further intensification: "*But it won't stop there. Because then they will say, 'Now we will go inside people's homes because someone can murder people inside there'"* (P4-I). The restriction on freedom was perceived as a potentially dangerous one not just for individual citizens but for all of society:

> *"Don't you see this as limiting your freedom? […] the thing that bothers me most about this is that it's very easy for someone to have control over the freedom of, we're not saying over just one person, you know, we're saying over the entire population. I think it's very easy to abuse something like this" (P7-I).*

Nevertheless, one of the participants proposed a counter-argument to the notion that intensive surveillance would pose limitations to citizens in their everyday life; underscoring the 'caring' function of surveillance, she argued as follows:

> *"You're saying you're limiting my freedom. On the contrary, I feel freer because I can do what I like, if I'm doing things that are well intentioned, see? If I feel like wrecking somewhere today, I can't do it, see? But instead I feel freer to do whatever I want; I know that if something happens I would be safe because there's someone watching. You can see it this way, as well (P6-I*).

Feelings of vulnerability and insecurity were also attributed to a possible shift in the political scene; some participants argued that should a change in the national political scene occur, methods of intrusive surveillance could potentially be used against the interests of citizens:

> *"What bothers me most is that it starts out as something harmless, for your safety, for your security, but, you never know do you? Alright, maybe you'll tell me I'm thinking of some science fiction film, but in life you don't know what developments there will be, [in] the political scene, and how these things can then be used, eventually, against the population. So that's why I get a very uncomfortable feeling about these things" (P5-III).*

When considering the possibility of political developments, others similarly expressed their concerns about potential consequences: *"[…] too many risks are involved. There are too many things that can go wrong"* (P4-I). Furthermore, other threats which appeared to increase the participants' vulnerability included those related to the misuse and misappropriation of personal data collected by smart surveillance and dataveillance: "*You try to do something good with technology but then because of misuse or because people hack into it [the system], you're not safe"* (P6-I). Concerns about possible consequences where voiced by several participants: *"Let's me make it clear, there's a good and a bad element in everything. And then you start thinking, but then if these things develop, how will they be used? And will it turn out to my detriment, eventually?* (P5-III).

Participants additionally discussed their views on the effectiveness of surveillance for purposes of law enforcement. Most participants acknowledged that the use of technology could be somewhat useful for purposes of investigation, *"We can backtrack to see what happened"* (P1-III) and, consequently, for the possible identification of the culprits: *"It would make it easier to catch the person"* (P5-III). In contrast, opinions on whether surveillance would be effective in terms of prevention were rather mixed. While some participants stated that to a certain extent certain crime might be prevented by the use of surveillance measures, others argued that surveillance will not act as a deterrent:

> *"I think that technology and CCTV, or whatever, don't give you security. [...] It's society that gives you security, your environment, because with CCTV and with all the security measures there will still be murders, there will still be kidnappings […] I don't know how much of a deterrent it is […] (P2-III)*

Consequently, a number of participants challenged the notion that surveillance can, in and of itself, guarantee security, especially due to the belief that individuals will find the "ways and means" to somehow evade surveillance:

> *"This is how I reason things out. It's a cat and mouse game. In the sense that the stronger the surveillance, the more savvy the criminals will become. So they are still going to find ways and means, crime isn't going to end. They will find other ways so it will be a never ending game (P10-II).*

Similarly, another participant stated: *"Isn't it obvious that the criminal will be on the alert and will remain one step ahead? You're not going to eliminate crime, that's for sure"* (P9-II). Thus, the predominant belief amongst participants, even those who appeared to be generally in favour of surveillance, was that security could never be fully guaranteed: *"To eradicate things completely is impossible […] you have to be realistic"* (P1-I). In light of this, a prevalent belief that emerged mainly in

Group 1 (18-24 years) and Group 3 (45+ years) was the notion that surveillance should not be regarded as a panacea to security-related concerns; in fact a number of participants argued strongly for the use of education, rather than an intensification of surveillance:

> *"I think these things cost a pretty penny. If these – I come from the social sector – if the government invested these funds to educate people wouldn't that be better than monitoring everybody and seeing where they are? Wouldn't it be better to provide education instead?" (P5-I).*

5.3.2 Perception of Different Technologies

During this part of the discussion, the participants were asked about whether the use of the different technologies listed in the scenario is acceptable and whether such acceptance is contingent on any factors. Views on the different types of surveillance technologies were rather mixed in the different groups; nevertheless, some general patterns could be noted. With some exceptions, video-surveillance in public places was generally deemed acceptable, while views on the use of biometric data differed widely. In contrast, most participants regarded electronic tagging as extremely controversial, with only a minority of participants considering the use of this method as acceptable.

5.3.2.1 Video-surveillance

The use of video-surveillance was subject to different opinions throughout the three groups and in general it appears that acceptance was contingent on the particular situation: *"the context makes a big difference*" (P4-III). More specifically, participants' opinions differed according to whether such monitoring was taking place in a public or in a private space, and also on whether the location was considered as a *"very high risk area"* (P1-III) such as airports: "*Normally, in areas which are going to be high targets for terrorism. You would probably want this visible security to feel safe"* (P4-III).

Firstly, several participants expressed their agreement with the use of CCTV systems in public places and it appears that such acceptance might be partly attributed to the covert nature of video-surveillance: *"But one doesn't really notice […] it doesn't even bother you, you don't even think about it"* (P4-III). Additionally, several participants argued that the use of CCTV is so extensive and commonplace that eventually as a citizen *"you get used to it"* (P5-II), thereby underlining the normalisation of video-surveillance. Nevertheless, even amongst those who, in principle, agreed with the use of video-surveillance in public spaces, there were some who argued that such use should not be unrestricted: *"In certain places, maybe yes to having CCTV cameras, for example parks where certain things might happen, I mean. However, I still don't think they should be everywhere"* (P1-III).

In contrast to the above views, others appeared bothered with being monitored in public spaces: *"I have some reservations about having CCTV cameras in public places"* (P5-III); it appears that this was mostly due to the perception that their privacy was being breached. Similarly, others felt very strongly

about surveillance in public places and expressed their frustration, and at times even anger, at being constantly surveilled: *"I don't know why but I find it really irritating […] whenever I see a CCTV I feel a certain anger because we're being monitored […] you can't enter any street because you're monitored, you're monitored all the time" (P5-I).* Participants appeared to imply that this sense of frustration was, in part, due to the lack of choice citizens have in being monitored in public spaces: "*CCTVs outside bother me. Inside, in private I mean, if I entered a supermarket and there is CCTV, I understand. But outside, out in the street, in public places, [it bothers me]. In private places it's up to me, if I don't like it I don't enter"* (P2-III).

Participants from Group 3 (45+ years) also discussed the effectiveness of video-surveillance for law enforcement purposes, and once again, opinions in this regard varied. While some categorically stated that the use of CCTV is futile for purposes of preventing crime: *"[The use of] CCTV isn't going to reduce crime*" (P2-III), others argued that video-surveillance could, to a certain extent, have a positive effect: *"I think that CCTV does actually reduce crime a little bit, let's say that sort of crime, [such as] spontaneous types of acts where people would think twice before doing something"* (P5-III). On the other hand, the majority of participants appeared to believe that video-surveillance plays a useful role in the investigation of crime.

Participants also briefly discussed the use of the automatic number plate reader (ANPR) and the use of sound sensors. Similar to the use of video-surveillance, participants' opinions on the former monitoring method differed; while some categorically expressed their agreement with the use of ANPR: *"I agree with it, I don't see anything wrong with it"* (P7-I), others made it clear that their agreement was contingent on purpose of use: *"The number plate thing doesn't bother me […] as long as it only gets used for that [security reasons]"* (P1-I). On the other hand, some participants perceived the use of ANPR as *"a total invasion of privacy"* (P4-II). With regards to effectiveness for law enforcement purposes, it appears that while participants perceived ANPR as useful for purposes of investigation and prosecution, they perceived this technology as futile in terms of prevention of crime. Lastly, while the use of sound sensors was considered acceptable by some of the participants, others pointed out that the use of this technology could prove to be *"impractical"* (P1-III).

5.3.2.2 Biometric surveillance and electronic tagging

The use of biometric data and electronic tagging – hence surveillance involving the physical sphere – was also subject to mixed reactions. Some participants from Group 1 (18-24 years) and Group 2 (25-44 years) and the majority of participants from Group 3 (45+ years), regarded the use of these measures for surveillance purposes as particularly excessive: *"That's all too exaggerated in my opinion"* (P5-II). As mentioned previously, some argued that methods of intrusive surveillance could be counter-productive and that instead of providing a sense of security, such methods would instill fear in citizens: *"I think they're extreme. And with extreme measures people get frightened, and that is scary – when you put fear into people, it's scary"* (P1-III). In line with this view, these participants objected strongly to these measures, most especially to the use of electronic tagging:

> *"If it was up to me, I would only go as far as CCTV in that scenario. I would definitely draw the line at DNA, fingerprinting, iris scanning, definitely not tagging, regardless I mean of age, or anything. In fact there are cases in America where they are tagging children inside the school. And the children are trying to fight it very hard because they don't want it" (P4-III).*

The participants not only underscored the *"complete invasion of privacy"* (P4-III) resulting from the use of such measures, but also the loss of freedom that this would entail for the persons concerned: *"Basically you're always on a leash"* (P4-I). Additionally others challenged the use of electronic tagging on grounds that this could lead to a sense of dehumanisation:

> *"What bothers me the most is the electronic tag. I would never want to be just a number […] we read Margaret Atwood's' The Handmaid's Tale' for my class, and the fact that you're reduced to a number is very demeaning. So, yes, I prefer to have a camera on me all the time than have a chip in my body or a tag […] I'd become paranoid with fear in that case (P8-I).*

In particular the tagging of children was especially subject to debate. Firstly, some participants considered this as being totally unacceptable since they argued that this monitoring method would be detrimental to children's psychological development: *"I think it [electronic tagging] would limit your life in many things […] Imagine having our children tagged, from a young age, and they grow up with that mentality. They would grow up as if they have no freedom"* (P5-III). Moreover, the use of this surveillance tool was perceived as instilling a "culture of fear", one which would have ramifications for society at large: "*Because then you start having a culture of fear won't you? And a culture of fear is very insidious, because then it can be unstoppable"* (P1-III). In contrast, some participants, mainly from Group 2 (25-44 years), did not object to the use of electronic tagging*: "I don't think I would object to that"* (P1-II). In this regard one participant argued that, as a parent, tagging your own children *"would provide a certain [sense of] security, it would put your mind at rest"* (P3-II). With regards to the electronic tagging of elderly people, while the participants strongly opposed mandatory tagging, it appears that if this monitoring tool was *"not forced"* (P8-I) on elderly citizens but instead was a personal choice, it was then considered as acceptable: *"If it's something voluntary then it is your own business isn't it? It's your decision"* (P1-I). Moreover, participants generally agreed that the use of tagging could be beneficial for elderly people suffering from particular conditions such as dementia.

Lastly, views on the collection and use of biometric data also differed widely; while some participants appeared to find the use of biometrics acceptable on the premise that *"I don't have anything to hide"* (P2-I), others were totally against biometric surveillance and questioned such a request, especially in relation to the collection of a DNA sample: *"Why should I give my DNA?"* (P10-II). Moreover, participants were keen to point out the risks, as well as the advantages, of biometric surveillance, which appeared to have an influence on degree of acceptance. In particular, one of the uses mentioned by some was the use of DNA for the investigation of crimes: *"I agree with the one about DNA too because a lot of crimes get solved through this"* (P1-II). With regards to possible risks, some participants

appeared concerned that once collected and stored, biometric data could be misappropriated: *"What if my fingerprint is reproduced at a crime scene?"* (P2-I).

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' views on the effectiveness of the Data Protection Act and their opinions on length of data storage.

5.4.1 Effectiveness of laws and regulations

The predominant sentiment amongst the participants appears to indicate that they do not feel sufficiently protected by the current legislation. Albeit some perceived the Data Protection Act as being *"sort of helpful"* (P4-I), the participants unambiguously argued that this legislation *"needs to be improved further"* (P5-I). In this regard, a main point raised by one of the participants was that for laws to be effective they need to be *"changed and tweaked"* (P1-I) on a regular basis so as to reflect the fast pace of technological development: *"Because every two years the technology changes, practically, and the amount of data collected changes, the methods used to collect and process data change as well"* (P1-I).

Moreover, in all focus groups, the participants highlighted what they considered as two major problems influencing the effectiveness of the Data Protection legislation: a lack of enforcement and the existence of loopholes. First, the majority of participants highlighted what they perceived was a dire lack of enforcement by the authorities: *"[…] and it only gets enforced if you complain to the [Data Protection] Commissioner. As for the rest, they don't look for people breaking the law so that needs some improvement"* (P1-I). In relation to this, some of the participants appeared disgruntled that no legal action is taken in cases of data protection breaches: *"The Data Protection Commissioner just tells them "Don't do it again". And he has the means to impose fines but he doesn't all the same"* (P1-II). Secondly, in addition to issues of enforcement, the participants also pointed out that the legislation can be *"very easily circumvented"* (P1-I) since it has *"too many loopholes"* (P4-I). In light of these issues, several participants were extremely critical of the Data Protection Act and argued that this legislation is simply ineffective: *"I think it's a joke. Because whoever wants to access certain data, and provides a valid reason, a valid justification, they can […] if you are savvy and know what steps to take, you will gain access to the data. So it's a joke"* (P5-III). Nevertheless, a minority of participants claimed that they do feel protected *"to a certain extent"* by the legal mechanisms currently in place:

> *"There wasn't a law before and now there is a law to protect you so that if someone were to abuse of a particular situation, you can actually take legal action […] before you could do nothing. So to a certain extent I feel protected (P3-III).*

Overall, the above views appear to indicate that several participants have a low level of trust in the Maltese judicial system: *"I feel that many of the laws are there simply to be there rather than to be implemented"* (P6-III).

5.4.2 Length of data storage

Participants were also asked about their opinions on the length of storage of surveillance data and although some appeared hesitant in indicating a specific time frame, others offered a number of suggestions. Firstly, some participants argued that unless *"an incident"* (P3-III) happened, surveillance data should be disposed of after a specific time frame: *"[…] if for instance you have an entire week when nothing happened, all you have are people passing by, why should you keep a record of all that?"* (P1-I). In contrast, others argued that surveillance data should be kept for a longer period for any possible use which may arise in the future, such as in cases of crime investigation:

> *"Honestly, I think it should be kept depending on its importance, for instance they might not need to know what number plate I had on a car after 50 years would have passed, but as for DNA and fingerprints, they will keep those for as long as you live (P10-II).*

In relation to specific storage periods, participants mentioned time frames ranging between one week and six months, while others even agreed to an indefinite length of storage: *"If the problem isn't storage, I see no problem with leaving the data [stored] there"* (P6-I). In contrast, others were adamantly opposed to the storing of data: *"No, I don't think it should be kept"* (P10-II). In this regard, some participants were keen to point out that once data is stored, it could potentially *"fall into the wrong hands"* (P4-I).

6. Conclusion

Maltese participants displayed a high awareness that individual citizens are indeed the subjects of surveillance in commercial, boundary and public spaces. The results indicate that surveillance in these spaces has undergone a process of normalisation, and technologically-mediated surveillance in these contexts is regarded as mostly acceptable for security-related purposes as well as for marketing purposes in commercial spaces. On the other hand, surveillance through the use of mobile devices and virtual spaces appeared to bring up ambivalent feelings amongst the participants; while it was perceived that mobile phone usage can have a detrimental effect on privacy, most of the participants agreed that this type of monitoring could be a useful tool in certain situations, such as for law enforcement purposes.

While the majority of participants believed that massively integrated dataveillance is undoubtedly technically possible, they were of the opinion that legal restrictions and ethical concerns would prohibit the massive integration of personal data. Moreover, a number of participants expressed a strong belief that the extent of dataveillance would be dependent, in part, on individuals' self-responsibility in divulging their personal data. This was perceived to be especially the case where online behaviour was concerned, in particular when using social networking sites. In light of the ethical concerns raised by the participants, integrated dataveillance was generally considered unacceptable due to the belief that this practice poses a threat to citizen privacy. Nevertheless, albeit participants argued that dataveillance carries a number of risks, including the possibility of misuse and misappropriation of surveillance data, some participants also suggested a number of possible advantages, including user convenience. Overall it appears that acceptance was contingent on several criteria including purpose of use, whether consent was given, type of data to be collected and shared, and whether the type of entity involved in data collection and sharing was a state entity or a private company.

The majority of Maltese participants strongly questioned, upon reflection, the use of extensive surveillance for the sake of security, especially since they argued that security could never be fully guaranteed, even with the use of smart surveillance: "*I think there is always a way around it*" (P10-I). While most participants acknowledged that the use of technology could be useful for purposes of investigation, at the same time they expressed scepticism with regards to the use of surveillance technologies for the prevention of crime. Intensive methods of surveillance were not only perceived as violating citizen privacy but also as providing a powerful tool to control citizens and to restrict individual freedom. Nevertheless, in contrast to the predominant sentiment, a minority of participants appeared to feel reassured with the presence of surveillance measures and stated their willingness to sacrifice their privacy for more surveillance in case of an increase in the level of threat.

On a last note, most of the participants expressed their reservations with regards to the extent of protection offered by the Data Protection Act and argued that, in addition to addressing current loopholes, what is primarily lacking is enforcement in case of privacy breaches. Moreover, a number of participants added that it is simply not enough to focus on strengthening the legal mechanisms

currently in place: they argued that in conjunction with such changes, more effort should be invested in creating *"a greater awareness on the importance of privacy"* (P7-I). More specifically, participants stated that such efforts should be directed at educating people on how to be more cautious with their data: "*So what is important is that people are actually educated about these things so that they are informed that they shouldn't give away extra information"* (P5-III).

Acknowledgements

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

APPENDIX A – RECRUITMENT QUESTIONNAIRE

Section A

(A1) Gender

☐ Male
☐ Female

(A2) Age

☐ 18-24
☐ 25-34
☐ 35-44
☐ 45+

(A3) Would you say you live in a

☐ Metropolitan city
☐ Urban town
☐ Rural area

(A4) What is your highest level of education?

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

(A5) What is your occupation?

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

Section B

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

☐ Yes
☐ No

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

☐ Yes
☐ No

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

☐ Yes
☐ No

(B4) Do you drive a vehicle?

☐ Yes
☐ No

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

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

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

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

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

☐ Yes
☐ No

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

☐ **Yes**
☐ **No**

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

☐ Yes
☐ No

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

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

APPENDIX B

DISCUSSION GUIDELINES (ENGLISH)

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

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

[20min]

- *To explore participants' experience with surveillance & how they perceive it*
- *To explore participants' awareness and knowledge of the different surveillance technologies*

Aims:

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

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

3. Explore the participants' understanding of

Item 2

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

Scenario 1: Supermarket

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

Scenario 2: Travelling

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

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

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

Scenario 4: Mobile devices

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

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

1. ***How is the information being collected:***
    a. ***Which types of technologies do you think are used to collect your personal information?***
2. ***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?***

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

Presentation of MIMSI scenario to participants

[30mins]

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

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

Item 4

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

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

***Customer Care Agent**: Good morning this is Sharon speaking, how are you Mr. Brown? We were expecting your call after your work contract ended over a month ago.*
***Mr. Brown**: Erm...yes in fact that's why I'm calling...*
***Customer Care Agent**: Well, I'm actually not surprised you called now...how was your holiday in Cyprus? I am sure your wife and kids enjoyed the resort you were staying in...*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Aims
1. Participants' first reactions including:

Possibility / impossibility of scenario

1a. How would you feel if this happened to you?
(Also probe to establish the degree of control / helplessness felt by the participants in such a hypothetical scenario)

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

Acceptability / unacceptability of scenario

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Running Total: 1 hour 15min

Reactions to scenarios

[About 20mins]

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

Item 5

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

Due to an significant increase in ***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 <u>safe</u> in the scenario provided?
1b. What makes you feel <u>vulnerable</u> in the scenario provided?

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

2. Deployment of specific technologies

2. From the smart technologies depicted in the scenario, i.e.
CCTV with Automated Facial Recognition,
Automatic Number Plate Recognition (ANPR),
Sensors (with the ability to detect loud noises),
Biometric technologies (including fingerprinting) and
Electronic tagging (which uses RFID)
2a. Which technologies do you consider <u>acceptable</u>? Why?
2b. Which technologies do you consider <u>invasive</u> and as a threat to your privacy? Why?
2c. What do you think of these automated (or semi-automated) technolgies whereby the final decision is taken by the system and not by a human operator?
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?

3. Locations of deployment such as:
Airports
Malls
Streets

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

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

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

5a. What do you think about the length of storage of surveillance data? Does it make a difference?
To help you probe, provide the following examples to the

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

APPENDIX C – DISCUSSION GUIDELINES (MALTESE)

Introduzzjoni	*'Briefing'*
Merħba lill-parteċipanti - *Tislija lill-parteċipanti* - *Tqassim tan-'name tags'* - *L-iffirmar tal-formula tal-kunsens* -	*Ilqa' lill-parteċipanti eżatti kif jidħlu. Iggwida lill-parteċipanti lejn is-siġġu tagħhom u pprovdi 'name tag' lill-kull parteċipant.* *Qassam il-formula tal-kunsens lill-parteċipanti u itlobhom biex jaqrawha u jiffirmawha qabel ma jibda il-'focus group'. Dan huwa mportanti sabiex jigi żgurat li l-parteċipanti jifhmu għal xiex qed jagħtu il-kunsens tagħhom.*
Introduzzjoni [10 minuti] - *Ringrazzjament* - *Introduzzjoni tat-tim li ser imexxi d-diskussjoni* - *Għan* - *Kunfidenzjalita'* - *Tul ta' ħin tal-'focus group'* - *Regoli tal-grupp* - *Introduzzjoni tal-parteċipanti*	**Merħba għal dan il-'*focus group*' u qabelxejn grazzi talli qbiltu li tipparteċipaw f' din id-diskussjoni. Napprezzaw li tajtuna l-ħin prezzjuz tagħkom sabiex tipparteċipaw f'dan il-proġett u nixtiequ ngħidulkom li l-parteċipazzjoni tagħhkom għandha valur kbir għal din ir-riċerka.** **Jiena jisimni _____ u ser inkun qed niffaċilita din id-diskussjoni. Ser tkun qed tgħini _____ li bħala r-Relatur ser tkun qed tieħu n-noti ta' dak li jintqal u tirrekordja d-diskussjoni.** *F'każ li hemm kollegi ohra fil-kamra ntroduċihom ukoll.* **Id-diskussjoni ser tieħu bejn siegħa u nofs u sagħtejn, u minħbba li ser nirrekordjaw dak kollu li ser jintqal, nitlobkom titkellmu b'mod car; l-opinjonijiet u l-ħsibijiet tagħkom huma ferm importanti għal din ir-riċerka u għaldaqstant bl-ebda mod ma rridu nitilfu l-kummenti tagħkom.** **Kif diġa tennejt meta ħejtu kkuntattjati biex tipparteċipaw f'din id-diskussjoni, it-tema ta' dan il-'*focus group*' huwa t-teknoloġija u l-privatezza, u qed jiġi organizzat bħala parti mill-proġett SMART, li huwa ko-finanzjat mill-Kummissjoni Ewropea. Għal dawk fostkom li jixtiequ jsiru jafu iktar dwar il-proġett SMART, nitolbukom tinfurmawna sabiex intukhom iktar informazzjoni dwaru malli nikkonkludu l-'*focus group*'.** *Huwa mportanti li f'dan il-waqt, l-ebda dettalji ohra dwar il-kontenut tal-'focus group' ma jigu mogħtija sabiex id-diskussjoni bla ebda mod ma tiġi nfluwenzata.* **Kif diġa ġejtu nfurmati meta qrajtu u ffirmajtu l-formula tal-kunsens, dak kollu li ser jiġi rrekordjat waqt din is-sessjoni ser jinżamm kunfidenzjali u l-identita' tagħkom ser tibqa' anonima. Dan ifisser li l-kummenti tagħkom ser ikunu maqsuma biss ma dawk li huma nvoluti f'din ir-riċerka u jista jagħti l-każ ukoll li l-kummenti tagħkom ikunu wżati f'publikazzjonijiet xjentifici li huma relatati ma din ir-riċerka. Il-kummenti li ser jidhru ser ikunu**

	anonimizzati qabel ma jiġu ppubblikati, u għaldaqstant, bl-ebda mod mhu ser ikun hemm il-possibilita' li tiġu identifikati bħala parteċipanti. Filfatt, kull wieħed u waħda minnkom ser tingħataw numru u huwa dan in-numru li ser jintuża fir-rapport. **Qabelxejn, nixtiequ wkoll inkunu ċerti li lkoll tħossukhom komdi biżżejjed fil-grupp sabiex taqsmu l-opinjonijiet tagħhkom. Biex dan ikun possibbli, nixtieq insaqsi l-kull wieħed u waħda minnkom sabiex timxu ma' dawn ir-regoli li ġejjin:** ▪ **Nixtiequ li kulħadd jipparteċipa - aħna nteressati fl-opinjoni ta' kull wieħed u waħda minnkom** ▪ **M'hemmx tweġibiet tajbin jew ħżiena, jiġifieri ejjew ilkoll naqblu li ser nirrispettaw l-opinjoni ta' xulxin** ▪ **Nitlobkom tpoġġu l-'*mobile*' fuq '*silent*' sabiex id-diskussjoni ma tiġix interrotta** ▪ **L-opinjoni ta' kulħadd hija mportanti u għaldaqstant nitolbukom biex tagħtu l-kummenti tagħkom wieħed wieħed. Ejjew nifthemu biex ma nitkellmux fl-istess waqt, inkella ser ikun diffiċli għalina biex insegwu dak kollu li jintqal waqt id-diskussjoni.** ▪ **Ejjew naqblu bħala grupp li nirrispettaw il-kunfidenzjalita' ta' xulxin sabiex kulħadd ihossu komdu biżżejjed li jitkellem b'mod ħieles.** **Jekk hawn xi ħadd li jixtieq jissuggerixxi xi regoli oħra, ħossukom liberi li taqsmuhom ma l-grupp.** **Hawn xi ħadd li għandu xi mistoqsijiet qabel nibdew?** **Tajjeb, mela biex nibdew ser insaqsikom biex tintroduċu ruħħkom fil-qosor lill-bqija tal-grupp mingħajr ma tikxfu informazzjoni privata. Ejjew induru dawra mal-grupp sabiex tgħidulna isimkom u forsi xi haga żgħira fuqkom. Ħa nibda jiena... *(introduċi lilek innifsek fil-qosor)*** *Ħin: 10 il-minuta*
Oġġettivi **Ezerċizzju tal- '*word association*'** **[5 minuti]** - *Logħba li sservi bħala 'ice-breaker'* - *Sabiex jinħolqu assoċjazzjonijiet spontaneji mat-temi prinċipali* - *Isservi bħala bidu għad-diskussjoni*	**Temi ta' diskussjoni u eżerċizzji** ***Eżerċizzju nru. 1*** **Biex nibdew, ser nagħmlu eżerċizzu: Ser naqra kelma u nixtieq li tgħiduli l-ewwel ħaġa li tiġi f'moħħkom meta tisimhu l-kelma. Ha nippruvaw eżempju qabel: X'inhi l-ewwel ħaġa li tiġikhom f'moħħkom meta tisimhu l-kelma 'ikel'? Jekk jista jkun, aħsbu f'kelma waħda jew frasi qasira, u mhux sentenzi twal.** *Aqra (waħda wara l-ohra): Teknoloġija, privatezza, sigurta' nazzjonali, informazzjoni personali, sigurta' personali* *Ħin: 15 il-minuta*

Diskussjoni fuq esperjenzi ta' kuljum relatati mas-sorveljanza

[20 minuta]

- *Espolarazzjoni ta' l-esperjenzi tal-parteċipanti f'dak li għandhu x'jaqsam mas-'sorveljanza' u l-perċezzjoni tagħhom dwarha.*

- *Esplorazzjoni tal-livell ta' għarfien tal-parteċipanti fir-rigward it-teknologiji differenti ta' sorveljanza*

Għanijiet:

1. *Esplora l-livell ta' għarfien tal-parteċipanti rigward it-teknologiji*
2. *Esplora l-esperjenza ta' monitoraġġ tal-parteċipanti fir-rwoli differenti tagħhom*
3. *Esplora l-ħsibijiet tal-parteċipanti rigward fejn qiegħda tispiċċa*

Eżerċizzju nru. 2

Ejjew nitkellmu dawr xi ħaġ'oħra. Nixtieqkom taħsbu f'mumenti li f'waqthom tħossu li inthom jew dak li qegħdin tagħmlu qed jiġi osservat. Barraminnhekk, nixtieqkom taħsbu wkoll f'mumenti fejn inthom konxji li nformazzjoni dwarkom qed tiġi miġbura. Ejjew nibdew billi naħsbu f'dawk l-affarijiet li nagħmlu fil-ħajja tagħna ta' kuljum. Li ġejjin huma ftit eżempji ta' sitwazzjonijiet li niltaqgħu magħhom.

Xenarju nru. 1: '*Supermarket*'

Bħala l-ewwel eżempju nistgħu nieħdu xirja fis-'*supermarket*'. Xi ħsibijiet għandhom fuq din is-sitwazzjoni?

Xenarju nru. 2: Vjaġġar

Ejjew niddiskutu sitwazzjoni oħra, din id-darba relatat ma' l-ivvjaġġar. X'taħsbu fuq meta nivvjaġġaw bl-ajru?

Xenarju nru. 3: Post pubbliku (ezempju mużew, '*stadium*')

Issa mmaginaw li qegħdin iżżuru post pubbliku, bhal per eżempju meta tmorru f'xi mużew jew tattendu xi attivita' bħal logħba futbol jew kunċert. X'tip ta' attivitajiet taħsbu li jkunu qed jiġu rrekordjati hawnhekk?

Xenarju nru. 4: Il-'*mobile*' u apparat simili

Ejjew niddiskutu eżempju ta' l-aħħar. Aħsbu fid-drabi li tużaw il-'*mobile*'. X'taħsbu li qed jiġi rrekordjat f'dan il-każ?

Għal kull waħda, kif ukoll fejn huwa relevanti, esplora fid-dettal il-punti li gejjin:

1. ***Kif qeghda tingabar l-informazzjoni:***
   a. ***X'tip ta' teknologiji taħsbu li qed jintużaw sabiex tinġabar l-informazzjoni personali tagħkom?***
2. ***It-tip t'informazzjoni li qiegħda tinġabar:***
   a. X'tip t' informazzjoni personali taħsbu li qiegħda tinġabar?
3. ***Min qed jiġbor l-informazzjoni:***
   a. Min taħsbu li huwa responsabbli għall-ġbir u l-monitoraġġ tal-informazzjoni personali tagħkom?
   b. Fejn taħsbu li qed tispiċċa l-informazzjoni personali tagħkom?

l-informazzjoni personali tagħhom 4. *Esplora l-ħsibijiet tal-parteċipanti dwar ir-raġunjiet għaliex l-azzjonijiet u l-imġieba tagħhom qegħdin jiġu osservati, ssorvelljati u miġbura.*	4. ***Għaliex l-informazzjoni qegħda tiġi rrekordjata, migbura u storjata:*** ***a. Għaliex taħsbu li l-informazzjoni personali qegħda tigi rrekordjata u miġbura?*** ***b. B'liema mod taħsbu li l-informazzjoni personali tagħkom ser tiġi użata?*** *Ħin: 35 il-minuta*
Turija ta' *'flashcards'* li juru t-teknologiji u l-istrumenti differenti ta' sorveljanza [10 minuti] - *Biex il-parteċipanti jiġu esposti għal numru ta' teknologiji u strumenti tat-tip 'SMART' sabiex il-parteċipanti jifhmu aħjar it-tema prinċipali u għaldaqstant id-diskussjoni timxi b'mod iktar faċli.*	***Eżerċizzju nru. 3*** *Ippreżenta t-tlett 'cards' (fejn kull waħda turi tipi ta' teknologiji u applikazjonijiet differenti) lill-grupp. Il-'cards' jinkludu l-istampi li ġejjin:* ***Card nru. 1 - 'Person or event recognition & Tracking Technologies'** : 'Automated moving of closed circuit television (CCTV) cameras'; 'Automatic number plate reader' (ANPR) jew 'Automatic vehicle number identification' (AVNI); u apparat ta' 'tracking' bħal 'mobile phone tracking' u 'RFID'* ***Card nru. 2 - 'Biometrics'**: Teknologiji u sistemi bijometrici bħal skanners tal-marki tas-swaba ('Fingerprint scanning') u tal-iris ('Iris scanning'); u l-immagini tal-wicc (Automatic facial recognition, AFR)* ***Card nru. 3 - 'Object and product detection devices'**: 'Knife arches' (portal) u apparat tar-raggi X ('X-ray devices')* *Ħin: 40 il-minuta*
Preżentazzjoni lill-parteċipanti tax-xenarju 'MIMSI' [30 minuta] - *Esplorazzjoni tal-ħsibijiet tal-parteċipanti fir-rigward tal-implikazzjonijiet tal-'MIMSI'* - *Esplorazzjoni tat-*	***Eżerċizzju nru. 4*** *Ipprezenta lill-grupp ix-xenarju ipotetiku li ġej. Tista' tipprepara reġistrazzjoni tal-awdjo ta' din it-telefonata minn qabel u tippreżentah lill-grupp.* ***Telefonata ma' Uffiċċjal tal-Customer Care fl-uffiċċju prinċipali tal-ETC*** ***Uffiċċjal: Bonġu, jiena Sharon, kif inti Sur Attard? Konna qed nistennew it-telefonata tiegħek wara li għalaqlek il-kuntratt tax-xogħol iktar minn xahar ilu.***

twemmin u l-attitudni tal-parteċipanti, kif ukoll kif iħossuhom fir-rigward ta' meta l-informazzjoni personali tagħhom tiġi mqassma lill-ħaddiehor	***Sur Attard: Erm...iva infatti għalhekk qed inċempel...*** ***Uffiċċjal: Biex ingħidlek m'inhix sorpriza li cempilt issa…kif mortu fuq il-btala tagħkom f'Cipru? Ċerta li kemm il-mara u kemm it-tfal ħadu gost fir-'resort' fejn qattajtu l-btala…*** ***Sur Attard: Iva kienet btala sabiħa…u inti kif taf dan kollu?*** ***Uffiċċjal: Heqq, din l-informazzjoni qiegdda fis-sistema tagħna Sur Attard....ovvjament. Ifhem, aħjar tibda' taħsiblu biex issib xogħol gdid…bl-ispiża tal-btala u l-ħlas tal-'loan' tal-karozza li daqt jasallek…biex ma nsemmux il-ħlas tal-VISA fit-tnejn u għoxrin ta' dan ix-xahar...*** ***Sur Attard: Din l-informazzjoni qiegħda wkoll fis-sistema?*** ***Uffiċċjal: Ħeqq mela Sur Attard. Qabel ma ninsa, għamilt għażla vera tajba fuq dak il-ktieb li xtrajt 'online'...jiena qrajtu u biex ingħdilek ħadt erba' ideat tajbin…*** ***Sur Attard: Hmmm...sewwa…riwgard dan is-servizz il-ġdid għat-tfittxija tax-xogħol, għandi bżonn intikom ritratt riċenti?*** ***Uffiċċjal: Le Sur Attard, m'hemmx għalfejn! Għandna diversi ritratti riċenti fis-sistema tagħna. Filfatt qed niftakar…x'naqra 'suntan' għandek wara dik il-btala! Nimmaġina li t-temp kien vera sabiħ! Eh bilħaqq, qabel ma ninsa, rigward ir-ritratt, x'tippreferi; wieħed bin-nuċċali jew mingħajr?*** ***Sur Attard: Hmmm...ifhem....mingħajr nuċċali tajjeb ta...issa....rigward ir-reġistrazzjoni, nistgħu nagħmlu appuntament xi ħin il-ġimgħa d-dieħla?*** ***Uffiċċjal: Ħa niċċekkjalek fis-sistema...x'taħseb għall-Erbgħa wara nofs in-nhar? Hmmm…żomm sekonda! Qed ninnota li għandek appuntament mat-tabib eżatti f'dak il-ħin. U ċerta li ma tridx titilfu għax aħjar tieħu ħsiebu dak il-kolesterol! X'taħseb fuq il-Ħamis l-ewwel ħaga fil-għodu, għad-disgħa?*** ***Sur Attard: Il-ħamis filgħodu tajjeb...hemm bzonn inġib xi dokumentazzjoni miegħi?*** ***Uffiċċjal: Le Sur Attard, l-informazzjoni li għandna bżonn qiegħda kollha fis-sistema tagħna.*** ***Sur Attard: M'għandix dubju...*** ***Uffiċċjal: Grazzi talli ċempilt Sur Attard u narawk il-gimgħa d-dieħla. U bilħaqq, gawdieh dak il-'cappuccino' ghand Café Cordina...*** ***Sur Attard: Qed ingawdieh... saħħa...***
Għanijiet *1. Ir-reazzjonijet tal-parteċipanti, inkluż:* *Jekk dan ix-xenajru huwiex possibbli / impossibli* *Jekk dan ix-xenarju huwiex aċċettabbli /*	*Wara li x-xenarju gie ppreżentat lill-grupp, esplora fid-dettall il-punti li ġejjin:* ***1a. Kif iħossukom kieku jiġrilkom hekk?*** *(Hawnhekk esplora wkoll il-livell ta' kontroll jew nuqqas ta' kontroll li jinhass fost il-parteċipanti f'xenarju bhal dan.* ***1b. Kif iġġibu ruħhkom kieku jiġrilkom hekk? X'tagħmlu?*** ***1c. Xenarju bħal dan huwa possibbli / impossibbli?*** ***1d. Xenarju bħal dan huwa aċċettabbli / inaċċettabbli?***

inaċċettabbli	
2. *It-twemmin u l-attitudni tal-parteċipanti fir-rigward ta' kif it-tekonoloġija taffetwwa jew tista' taffettwa l-privatezza tagħhom.*	***2a. Kemm taħsbu li t-teknoloġiji ndividwali (dawk 'stand alone') jaffettwaw il-privatezza tagħkom?***
	2b. Kemm taħsbu li t-teknoloġiji tat-tip 'SMART' jiġifieri dawk li jipproċessaw id-dejta b'mod awtomatiku (jew kawżi awtomatiku) jaffetwwawa il-privatezza taghħkom?
3. *It-twemmin u l-attitudni tal-parteċipanti fir-rigward tat-tip ta' informazzjoni bħal: Rekords ta' natura medika; informazzjoni finanzjarja; ritratti u lokalizzazzjoni*	***3a. X'tip ta' nformazzjoni personali ssibu li hija aċċettabbli li tiġi miġbura, użata u mqassma lil ħaddieħor?***
	3b. X'tip ta' nformazzjoni personali toġġezzjonaw li tiġi miġbura, użata u mqassma lil ħaddieħor?
4. *It-twemmin u l-attitudni tal-parteċipanti fir-rigward ta' l-ġbir, l-użu u tqassim ta' nformazzjoni personali minn terzi persuni*	***4a. X'taħsbu dwar li l-informazzjoni personali tagħkom tiġi miġbura, użata u mqassma lil ħaddieħor mill-istat?***
	4a. X'taħsbu dwar li l-informazzjoni personali tagħkom tiġi miġbura, użata u mqassma lil ħaddieħor minn entitajiet privati (bħal dawk kummerċjali)?
5. *It-twemmin u l-attitudni tal-parteċipanti fir-rigward tal-vantaġġi u l-iżvantaġġi li jiġu sorveljati*	***5a. Taħsbu li hemm xi vantaġġi li l-azzjonijiet u l-imġieba tagħkom tiġi sorveljata?***
	5b. Taħsbu li hemm xi żvantaġġi li l-azzjonijiet u l-imġieba tagħkom tiġi sorveljata?
	Ħin: Siegħa u 15 il-minuta
Reazzjonijiet għax-xenarji	***Eżerċizzju nru. 5***

[20 minuta]

1. *Sabiex jinħoloq dibattitu u b'hekk jigu esplorati l-percezzjonijiet tal-parteċipanti dwar il-kompromess relatat mas-sigurta' u l-privatezza*

2. *Hawnhekk, id-diskussjoni m'għandiex tiffoka fuq jekk dawn it-teknoloġiji iżidu s-sigurta - dan għandu jiġi meqjus bħala fatt. Id-diskussjoni għandha tiffoka l-iktar fuq jekk dawn it-teknologiji għandhomx effett fuq il-privatezza u għaldaqstant tiffoka fuq il-kompromess relatat mas-sigurta' u l-privatezza.*

Għanijiet

1. *Il-klima ta' sigurta' u l-livell ta' riskju*
2. *L-użu ta' teknoloġiji speċifiċi*

Matul l-ezerċizzju li gej, ser inkunu qegħdin niddiskutu x-xenarju ipotetiku li ġej. Immaġinaw din is-sitwazzjoni:

Minħabba zieda sostanzjali ta' atti <u>vjolenti</u> kriminali fil-belt kapitali, inkluż <u>każijiet ta' htif u qtil li jidhru li saru fuq bażi każwali u li m'humiex konnessi</u>, il-gvern iddeċieda li jintroduċi CCTV cameras - li jiskennjaw l-immaġini tal-wiċċ - f'kull post pubbliku, kemm dawk li huma propjeta' tal-gvern (bħal subways, ġonna pubbliċi u '*public conveniences*') kif ukoll dawk li huma propjeta' privata (bħal ħwienet, '*shopping malls*' u taxis). Barraminnhekk, kull karozza li tgħaddi minn ċertu postijiet ewlenin ikollha n-numru tar-reġistrazzjoni rrekordjata. Qed jiġi ppjanat ukoll li jiġu nstallati numru ta' sensors f'kull post pubbliku li jkollhom il-kapaċita' li jgħarfu ċertu ħsejjes bħal fil-każ ta' meta persuna twerżaq. Kull ċittadin ser ikollu jagħti d-DNA, il-marki tas-swaba u l-immaġini tal-iris. Il-gvern iddeċieda wkoll li kull ċittadin li huwa meqjus bħala persuna li tista' tkun ta' riskju għal individwi oħra tkun itteggjata b'mod elettroniku sabiex il-movimenti tagħha jiġu ssorveljati. Minhabba raguni ta' sigurta', anki persuni anzjani u tfal ta' taħt it-tnax il-sena ser ikunu tteggjati b'mod elettroniku. Id-dejta kollha minn dawn it-teknoloġiji differenti ser tkun miżmuma ġo '*databases*' illinkjati li huma amministrati mill-puluzija, li jiġu nfurmati b'mod awtomatiku f'każ li jkun hemm lok għal tħassib u riskju għal kwalunkwe ċittadin.

Wara, għid lill-parteċipanti sabiex jimmaġinaw dan ix-xenarju pero bil-varjazzjonijiet li ġejjin:

Varjazzjoni nru. 1: Avolja kien hemm żjieda sostanzjali f'atti kriminali fl-ibliet ġirien tiegħek, fil-belt fejn toqogħod ma kien hemm l-ebda żjieda fil-kriminalita'. Madanakollu, il-gvern xorta ddeċieda li jintroduċi numru ta' miżuri ta' sorveljanza bħala prekawzjoni.

Varjazzjoni nru. 2: F'pajjiżek, ir-rata ta' kriminalita' hija ferm baxxa, pero l-gvern jiddeċiedi li jintroduċi numru ta' miżuri ta' sorveljanza bħala prekawzjoni wara li seħħ inċident isolat f'belt ġiriena tiegħek. Matul dan l-inċident, li seħħ ġo '*shopping mall*' raġel spara fuq numru ta' nies bil-konsegwenza li ġew midruba serjament.

Matul id-diskussjoni ta' l-ewwel xenarju u l-varjazzjonijiet tiegħu, esplora fid-dettall il-fatturi li ġejjin, u kif dawn il-fatturi jistgħu jaffettwaw il-kompromess relatat mas-sigurta' u l-privatezza.

1a. Biex iħossukom siguri fix-xenarju?

1b. Biex iħossukom vulnerabbli fix-xenarju?

1c. Kemm inthom lesti li tissagrifikaw il-privatezza tagħhom f'kaz li l-livell ta' riskju huwa differenti, bħal fil-varjazzjonijiet nru. 1 u nru. 2 tax-xenarju)

2. Mit-teknoloġiji tat-tip 'SMART' imsemmijin fix-xenarju, jiġifieri CCTV li tiskennja l-immaġini tal-wiċċ

	Automatic Number Plate Recognition (ANPR) ***Sensors (bil-kapaċita' li jgħarfu ċertu ħsejjes)*** ***Teknoloġiji bijometriċi (bħal marki tas-swaba)*** ***Electronic tagging (fejn jintuża l-RFID)*** ***2a. Liema huma dawk it-teknoloġiji li l-użu tagħhom huwa aċċettabbli? Għaliex?*** ***2b. Liema huma dawk it-teknoloġiji li l-użu tagħhom tħossu li huwa invasiv u li huwa riskju għall-privatezza tagħkom? Għaliex?*** ***2c. X'taħsbu fuq it-teknologiji li jiffunzjonaw b'mod awtomatiku (jew kważi awtomatiku) u li għaldaqstant id-deċizjoni aħħarijja tittieħed mis-sistema u mhux minn bniedem?*** 3. *Postijiet fejn tinsab is-sorveljanza* ***3a. Liema huma dawk il-postijiet li tikkunsidraw bħala aċċettabbli fir-rigward li tiġu sorveljati?*** ***3b. Liema huma dawk il-postijiet li tikkunsidraw bħala inaċċettabbli fir-rigward li tiġu sorveljati?*** 4. *Eżistenza ta' liġijiet u salvagwardji oħra (fir-rigward tal-gbir, ħażna u użu ta' nformazzjoni* ***4a. X'taħsbu dwar il-liġijiet tal-privatezza? Tħossukhom protetti b'dawn il-liġijiet?*** ***4b. Hemm xi salvagwardi jew fatturi / kundizzjonijiet oħra li kieku jserrħulkom raskom?*** 5. *It-tul ta' żmien li tinżamm l-informazzjoni / dejta ta' sorveljanza* ***5a. X'taħsbu dwar it-tul ta' żmien li tinżamm id-dejta ta' sorveljanza? Tgħamlilkom differenza?*** ***Bħala għajnuna biex tesplora iktar fid-dettal, agħti l-eżempji li jmiss lill-parteċipanti:*** - ***Ir-'recordings' tas-CCTV*** - ***Il-lokalizzazzjoni u l-movimenti ta' karozzi*** - ***Li jiġu miżmuma d-DNA, marki tas-swaba u l-immaġini tal-iris*** - ***Il-lokalizzazzjoni ta' ċittadini li huma ta' riskju għal oħrajn*** - ***Il-lokalizzazzjoni u l-movimenti ta' persuni anzjani u tfal*** ***5b. Jekk it-tul ta' żmien li tinżamm id-dejta tagħmel differenza, liema tul ta' żmien tikkunsidraw li huwa aċċettabbli?*** *Ħin: Siegħa u 35 il-minuta*
Oġġettivi	**Sommarju**
Sommarju tad-diskussjoni [5 minuti] ▪ *Biex tikkonferma mal-grupp il-punti ewlenin li ħargu mid-*	***Eżerċizzju nru. 6*** *Huwa utli li qabel ma l-'focus group' jigi konkluż, jingħata sommarju bil-punti ewlenin li ħarġu waqt id-diskussjoni. L-għan huwa li jingħata sommarju qasir fejn jissemmew it-temi u l-kwistjonijiet li gew imqajjma waqt id-diskussjoni. Wara, il-mistoqsijiet li gejjin jistgħu jiġu mpoġġija lill-parteċipanti:* - ***"Il-punti li semmejna issa kemm jirriflettu dak li ntqal waqt id-diskussjoni tal-lum?"***

diskussjoni ▪ *Biex tagħti cans lill-parteċipanti li jelaboraw fuq dak li ntqal*	- ***"Hemm xi ħaġa oħra li ma semmejniex?"*** - ***"Taħsbu li semmejna kollox?"*** *Waqt din is-sessjoni qasira, il-parteċipanti għandhom l-opportunita' li jesprimu l-ħsibijiet tagħhom u jistgħu wkoll jelaboraw fuq punti li jista' jkun issemmew fil-qosor waqt id-diskussjoni, iżda li għal xi raġuni jew oħra l-parteċipanti ma komplex jiddiskutu.* *Ħin: Siegħa u 40-il minuta*
Oggettivi	**Għeluq**
Għeluq tal-'focus group' [5 minuti] ▪ *Ringrazzjament lill-parteċipanti* ▪ *Għotija tar-rimbors* ▪ *Għotija ta' nformazzjoni fuq il-progett 'SMART'*	***Ezercizzju nru. 7*** **Ma dan l-ezercizzju, id-diskussjoni tagħna waslet fi tmiema. Nixtieq nieħu din l-opportunita' biex nerga' nirringrazzjakom talli attendejtu għal dan il-*'*focus group*'* **kif ukoll talli qsamtu magħna l-opinjonijiet, l-esperjenzi u l-ħsibijiet tagħkom.** *F'dan il-waqt, qassam ir-rimbors lill-parteċipanti u nforma l-parteċipanti b'dak li jmiss.* *Għati l-informazzjoni fuq il-progett 'SMART' lil dawk il-parteċipanti li jitolbu din l-informazzjoni.* *Ħin: Siegħa u 45-il minuta*

APPENDIX D – DEBRIEFING FORM

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

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

APPENDIX E – CONSENT FORM

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

Participation

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

Confidentiality and anonymity

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

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

Data protection and data security

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

Risks and benefits

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

Questions about the research

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

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

Signature: Date:

APPENDIX F – CODING MAP

1. Surveillance technologies in different spaces

1.1. Commercial space

1.1.1. Awareness of different surveillance methods/technologies

1.1.1.1. CCTV

1.1.1.2. Loyalty cards

1.1.1.3. Financial monitoring

1.1.2. Perceived purposes

1.1.2.1. Security purposes

1.1.2.2. Commercial reasons

1.2. Boundary (border) space

1.2.1. Awareness of different surveillance methods/technologies

1.2.1.1. CCTV

1.2.1.2. Smart CCTV with AFR

1.2.1.3. Biometric technologies

1.2.1.3.1. Fingerprinting

1.2.1.3.2. Iris scanning

1.2.1.4. Object and product detection devices

1.2.1.4.1. Luggage controls

1.2.1.4.2. Body scanners

1.2.1.4.3. Metal detectors

1.2.1.5. Monitoring of personal data

1.2.1.5.1. Passport control

1.2.1.5.2. Flight manifest

1.2.1.5.3. Airline booking system

1.2.1.6. Security staff

1.2.1.7. Sniffer dogs

1.2.1.8. Law enforcement officers

1.2.2. Perceived purposes

1.2.2.1. National security

1.2.2.2. Traveller safety

1.2.2.3. Commercial motivations

1.2.2.4. Collection of statistics

1.3. Common public spaces

1.3.1. Awareness of different surveillance methods/technologies

1.3.1.1. CCTV

1.3.1.2. Television cameras

1.3.1.3. Audio surveillance

1.3.1.4. Collection of personal data
1.3.1.5. Metal detectors
1.3.1.6. Security officers
1.3.1.7. Law enforcement personnel
1.3.2. Perceived purposes
1.3.2.1. Public security
1.3.2.2. Citizen safety

1.4. Mobile devices and virtual spaces
1.4.1. Awareness of different surveillance methods/technologies
1.4.1.1. Location tracking via GPS
1.4.1.2. Monitoring of call lists and message lists
1.4.1.3. Collection of data through smart phone applications
1.4.2. Perceived purposes
1.4.2.1. Law-enfocement purposes
1.4.2.2. Commercial purposes

2. Perceptions and attitudes towards smart surveillance and dataveillance
2.1. Feelings
2.1.1. Disbelief
2.1.2. Extreme discomfort
2.1.3. Anger

2.2. Behavioural intentions
2.2.1. Passive reactions
2.2.1.1. Immediate withdrawal
2.2.1.2. Emigrate
2.2.2. Self-protection strategies
2.2.2.1. Confront and investigate
2.2.3. Legal measures
2.2.3.1. Legal assistance
2.2.3.2. File a report to the Data Protection Commissioner
2.2.3.3. File a police report

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

2.3.1.2.1. Legal restrictions
2.3.1.3. Ethical aspect
2.3.1.3.1. Invasion of privacy
2.3.2. Acceptance of dataveillance
2.3.2.1. Purpose of use
2.3.2.1.1. Prevention and investigation of crime
2.3.2.1.2. Facilitation of user convenience
2.3.2.2. Provision of consent
2.3.2.3. Type of data stored and shared
2.3.2.4. Access to data
2.3.2.4.1. State
2.3.2.4.2. Private entities
2.3.2.5. Risks of dataveillance
2.3.2.5.1. Misuse
2.3.2.5.2. Misappropriation e.g. data theft
2.3.3. Perceived effectiveness of smart technologies
2.3.3.1. Decision-making capabilities of automated systems
2.3.3.2. Human agency
2.3.4. Perceived privacy impact of automated systems

3. Security-privacy trade-offs
3.1. Acceptance of technological surveillance
3.1.1. Feelings
3.1.1.1. Vulnerability and insecurity
3.1.1.2. Safety
3.1.2. General beliefs
3.1.2.1. Risks
3.1.2.1.1. Extreme form of control: association with a dictatorship and a police state
3.1.2.1.2. Visibility of surveillance heightens awareness to danger
3.1.2.1.3. Violation of privacy
3.1.2.1.4. Restrictions on freedom
3.1.2.1.5. Risks of further intensification
3.1.2.1.6. Misuse and misappropriation of personal data
3.1.2.2. Benefits
3.1.2.2.1. Safety and peace of mind: the “caring” function of surveillance
3.1.3. Effectiveness of surveillance
3.1.3.1. Ineffective/effective in offering protection and prevention
3.1.3.2. Effective for investigation purposes
3.2. Perceptions of different technologies
3.2.1. CCTV
3.2.1.1. Private and public spaces

3.2.1.2. High and low-risk locations

3.2.2. ANPR

3.2.3. Biometric data

3.2.4. Electronic tagging (RFID)

3.2.4.1. Considered as extreme

3.2.4.2. Strong perceptions of bodily/physical invasiveness

3.2.4.3. Sense of dehumanisation

3.2.4.4. Treat to privacy and freedom

4. Surveillance laws and regulations

4.1. Feelings and beliefs

4.1.1. Effectiveness of laws and regulations

4.1.1.1. Lack of enforcement

4.1.1.2. Existence of loopholes

4.1.2. Length of data storage