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

Marija Krlic[1], Noellie Brockdorff[2], Christine Garzia[2], Natalie Mundle[2]
[1] Department of Sociological Studies, University of Sheffield, Sheffield, UK
[2] Department of Cognitive Science, University of Malta, Msida, Malta

January 2014

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

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

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

Table of Contents

1. Key Findings

This document presents the UK 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 23 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 three focus groups conducted in the UK with 23 participants pointed to the following findings and features of citizens' knowledge and attitudes to the topics raised. Experience of surveillance measures is influenced by personal differences such as gender and age and this is an area worthy of more detailed exploration. Other personal differences - such as race, religion and place of abode or work - should also be empirically, comparatively and systematically researched. Attitudes to surveillance measures are highly nuanced and context-dependent. This makes conclusions and claims based on very general and broad-brush questions potentially dubious and unreliable.

Sufficient care must be taken, in this regard, when designing research instruments: if findings and claims are to be trustworthy, reliable and firmly based upon the data. Attitudes to surveillance were strongly held and influenced both acceptance of measures and perceptions of the organisations and agencies involved. The potential for serious mistrust and conflict to arise in relation to how their own and others' data was handled was evident. The sociological dimension to an evaluation of surveillance is critical and sociological analysis should be an essential component of the planning, design, implementation and review of any surveillance measure that is to be adopted for societal application.

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, and coordination and supervision of 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. In the United Kingdom these tasks were carried out by the University of Sheffield and University of Central Lancashire. The University of Sheffield carried out the data analysis and prepared this report.

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

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

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

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

3. Methodology

In total, 42 focus groups – three in each country – were conducted between February and November, 2013. Thirty-nine of the groups had between 6 and 10 participants, three groups had 11, 12 and 13 participants respectively. Overall, 353 participants took part in this research project. The focus groups in the United Kingdom were carried out on the 17th February, 2013; 20th February, 2013 and 27th March, 2013. The composition of the groups held in the United Kingdom 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.

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 C) at the end of each session.

All participants were required to read and sign a consent form (see Appendix D) 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. Notwithstanding this final version, the emergence of novel lower order codes was not excluded following the analysis of the remaining transcripts. The coding map for this report can be found in Appendix E.

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

4. Description of the Sample

The data analysis for the United Kingdom is based on a total of 23 participants of mixed age (from 19 to 85). The following box provides the details of group composition:

Participant number	Group 1 – 18-24 years	Group 2 – 25-44 years	Group 3 – 45+ years
P1	M	M	F
P2	M	F	F
P3	M	F	M
P4	F	F	M
P5	F	M	M
P6	M	M	F
P7	No-show	M	F
P8	No-show	M	M
P9	No-show	No-show	M
Total	**6**	**8**	**9**

Each focus group lasted approximately 2 hours. As earlier recruitment for a proposed pilot group had received a very poor response, a £10 shopping voucher was offered to participants and forwarded to them following the focus group in appreciation of their time and effort in attending. In the recruitment of participants difficulties were encountered in terms of finding a commonly suitable date and time; and, with the youngest age group, a third of agreed participants not showing up on the day without notification after expressing very positive motivation. The moderator had been reluctant to significantly over-recruit and risk 'turning people away at the door'; but, particularly with the younger age group, this is advisable in future to optimise participation levels on the day.

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.

Participants displayed a comprehensive familiarity with various surveillance technologies being applied in different spaces: such as, transport; retail; entertainment; and mobile communications. They readily described the availability of technologies, as well as their own experience of contact with them during the activities involved in these areas of life.

The participants accurately described the various purposes for which these technologies could be applied in the different spaces: distinguishing between national and border security; law enforcement and crowd control; commercial and financial; and administrative or logistical. They expressed an acknowledgement of the convenience these applications offered them in terms of the speed, ease and availability of goods and services. However, they also identified that this consumer-benefit entailed a trade-off: with a loss of privacy and control over their own personal data. As one discussant put it: "*Privacy is a privilege of the rich*" (P9-III).

Participants demonstrated an awareness of the numerous ways in which the range of these technologies were used - within the differing spaces - to collect and process diverse data; and how lucrative such data pools were and could be. They were aware of the potential and the availability of technical capacity for data to be linked, matched and mined; and they identified examples of where their personal data was being sold to third parties for secondary use. However, a large proportion of them did not appear to be aware that data matching and mining was actually happening on any notable scale. They, nevertheless, suspected that - as well as public agencies - large and even unknown, private bodies held the ability and inclination to do so, and this created a sense of vulnerability and mistrust.

Age differences were evident in this area: with the younger participants more readily using terms such as, drones, GPS and key stroke logging; being more familiar with features of the internet and social media; and much less indignant about perceived intrusions of their privacy; acknowledging that they had come to accept the pervasiveness of digitally-enabled monitoring and communication of information as it had been a prominent feature of their adult lives. As one younger respondent put it:

> "*It may be a generation thing. My Grandmother never lets her credit card out of her sight she will be following someone around a restaurant whereas I'm on on-line banking. I shop on-line all the time. I don't even think about it"* (P5-I).

5.2 Perceptions and attitudes towards smart surveillance and integrated dataveillance

One of the central tasks of this study was to research citizens' feelings and beliefs towards smart surveillance and massively integrated dataveillance, the latter referring to "*the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons*"[2]. In order to investigate the attitudes of participants, an everyday scenario was presented: 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 Negative feelings

Participants expressed a wide range of negative feelings associated with being data subjects and the focus of surveillance. However, this negativity was not in relation to smart surveillance per se, other than in the few instances where they identified its capacity to point to them as an individual and not as an anonymous body or unidentified member of a group/public.

The negative feelings, to varying degrees, largely comprised: lack of confidence; mistrust; powerlessness; fear; frustration; indignation; conflict and anger. These were initiated by perceptions of the following features associated with the application of the surveillance measures discussed:

- A blurring of boundaries: between public and private agencies' data handling; between primary, secondary and multiple re-use of data; and between security/law enforcement/administrative purposes and commercial/financial interests;

- A tokenistic and disingenuous approach by service providers to the importance of consent as a principle for data collection and processing;

- An assumption by data controllers that they could do, subsequently, what they wished with personal data they had collected as part of providing a service to the data subject;

- A lax view of the importance of the primary purpose for data collection - as a significant component of data subjects' consent - in relation to determining the subsequent processing of that data;

[2] Clarke, R. (1997).

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

- A dominance of financial and commercial interests in motivations for data sharing and processing decisions;

- The potential for errors, exclusion or discrimination to occur - without corresponding and reliable safeguards for prevention and rectification - particularly in relation to vulnerable groups, such as the unemployed;

- The impotence of legal and regulatory frameworks to ensure compliance: in the face of powerful interests that employ means to manipulate or circumvent provisions;

- The potential for repressive or undemocratic political interests - or even persecution - to be brought to bear: for example, in the event of a regime change;

- The added intrusiveness experienced with new technology: such as, with location tracking or enhanced CCTV capabilities (for example, with GPS or ANPR) where an individual's precise whereabouts, activities and associates could be identified and stored.

A number of statements from participants illustrated the nature and extent of these negative feelings and can be gauged from the following selection of direct quotes.

"*In those days we had the trust* [in the police] *to think that that surveillance was used correctly, the trust has gone nowadays and we've got this mistrust"* (P8-III).

"I am not comfortable that companies obtain my address from other lists and contact me at home" (P5-I).

"I have a general lack of trust in the data security. I worry about the amount of people that know where I am as a result of my mobile phone being in certain places" (P1-I).

"Knowing that they have all this information and know all these extra things about you, [I] wouldn't be happy. I mean I'd almost cynically expect them to start collecting stuff like that but I wouldn't consider it acceptable at all" (P5-II).

"Why should they make money out of your personal details that they have on you" (P3-II).

"There's a lot of that leverage that you have to submit your details and I feel I don't have any choice to use the technology or the website or whatever" (P8-II).

5.2.2 Personal differences in negative feelings

Some negative feelings were expressed more frequently and/or to greater intensity by older or female participants, respectively. Older participants, as has already been mentioned, expressed greater indignation at intrusions of their privacy, such as with telephone cold calling. As one participant in her seventies put it: "*We rang BT and told them about it and she said that shouldn't be happening. Well, I said, it is. She said just put the phone down. But you've got to get up and answer the phone haven't you"* (P1-III). She was swiftly supported by an 85 year old participant stating: "*And you know that someone's got that number when they shouldn't have it at all"* (P7-III).

Female participants expressed heightened sensitivity to issues involving the body/ physical and to health-related data. One participant used graphic wording to illustrate her point with regard to physical surveillance measures, stating: "*What about an airport. Whenever I go through I'm a bleeper and I've got some woman groping me, making me feel as if I've done something wrong, making me think I've got eyebrow tweezers in my pocket*" (P4-II). Another expressed concern at the suggestion that her medical data could be shared or seen: "*I'd be worried if someone knew why I'd been to see my doctor. That should be private between me and my doctor and I wouldn't imagine that someone would be able to get that information"* (P3-II).

Male participants also expressed a view that medical data was particular or special, but not with the same degree or quality of personal sensitivity as female participants. Rather, the males described how this information was of concern given its potential influence in terms of their desirability for employment and insurance approvals.

A further contrast between the genders was revealed when a male participant described how he advocated the installation of CCTV in the gym changing room following his locker being broken into. A female participant quickly countered that: "*I wouldn't want it anywhere like a changing room"* (P4-I); and was just as swiftly supported by another, stating: *"I agree*" (P5-I). A further area of concern for female participants surrounded their sense of personal safety, which, they recognised, could be both enhanced and eroded by data monitoring and sharing. In this case of negative feelings, one young woman stated that: *"On social networking someone found my name, address, who I lived with and that really, really scared me*" (P4-I). Another then added: *"Someone I know chose their secretary based on their Facebook photograph and that really annoyed me*" (P5-I). Most of the participants (male) laughed spontaneously at this revelation.

Negative feelings around surveillance issues emerged strongly during the focus groups. They were highly nuanced and largely context dependent. They also differed across age groups and gender differences. It may well be the case that other personal differences are important for this analysis - such as, race and ethnicity, socio-economic status, region or locality and religion - but, as age and gender were the only features to be identified within the groups' composition, this was beyond our current remit.

5.2.3 Positive feelings

Participants acknowledged that - as consumers, clients and travellers - they enjoyed the convenience that resulted from digitalisation of processes linked to the delivery of services. Provision of goods and services was - in many cases - swifter, cheaper and tailored more to their personal preferences as a result of digital data collection and analysis. Participants recognised that they 'traded' access to their personal data for enhanced convenience.

Participants also expressed an appreciation of the potential for enhanced health and safety that was offered by the use of modern technology. This comprised the following applications: electronic medical records that allowed health care personnel to treat them more effectively if they were away from home; CCTV monitoring in spaces where there was a greater likelihood that they may be a victim of crime; and electronic monitoring or 'tagging' of proven sex offenders or elderly sufferers of dementia. Participants, nevertheless, stated that this acceptance of the positive features of surveillance was not unconditional. They recognised the potential for misuse of both technology and data and, so, stipulated that activities must be appropriate and properly targeted and not arbitrary or unfair.

5.2.4 Personal differences in positive feelings

There was a contrast in the comments of female and male participants in relation to positive feelings of safety emanating from the application of surveillance techniques. The female participants more clearly and readily described how CCTV and GPS made them feel safer, particularly when alone at certain times or in isolated places or vulnerable situations. One participant added that she felt reassured that DNA would enable authorities to determine a victim's actual identity in an extreme case of murder or fatal incident: so that the family could be assured that they had received the return of the body of the correct person.

5.3 Behaviours and intentions

Despite a comic stereo-type of the British people never complaining about the quality of goods and services (especially in restaurants), participants displayed a readiness to complain in relation to the job centre scenario, following which they were asked directly about what action they would take. Given that organisational complaints procedures are well-developed and widespread in the UK context, it is, perhaps, unsurprising that participants said they would complain to the employee's supervisor or manager and, in a couple of cases, a newspaper and the M.P. They did not leap to the level of legal challenges or seeking legal interventions. More surprising, though, was the lack of knowledge, across all participants, not only of legal provisions, but also of any bodies or sources of advice and assistance with data protection issues. They seemed to be totally unaware of the existence of the ICO or particular civil liberties and lobby groups. As one participant put it: "*I would make a complaint to the job agency, unless there's an ombudsman or something"* (P4-I).

A significant feature, related to behaviours and intentions and expressed by participants in connection with data and surveillance, was that of passivity. They themselves acknowledged that, alongside a lack of knowledge of data protection laws and regulatory provisions, they were also insufficiently motivated or focused to follow particular instances of irritation and discomfort through to challenging actions or making a complaint. Younger participants described how the pervasiveness and frequency of contact with modern forms of surveillance and communication practices, which were an inherent feature of their adult lives, made them more complacent and accepting of them as being, in some way, inevitable. This was compounded by the fact that, if one didn't comply with the processes and data collection 'requested', access to the goods and services was denied. As one participant described it*: "There was that restriction, I was not allowed to find out unless I agreed with the terms of the website"* (P1-II).

5.4 Beliefs about current and future smart surveillance and massively integrated dataveillance

Participants expressed a belief that the job centre scenario was not currently realistic, as that agency would not have the access to or the capability for combining the disparate sources of information illustrated. However, they recognised that it was technologically possible to do so and, therefore, not unrealistic to consider it feasible for public agencies of the future. They also recognised that more powerful and sophisticated uses of technology were operated in some quarters - for example, GCHQ and specialist law enforcement units - but they still believed this to be targeted and not general surveillance. Therefore, it did not include them as they were ordinary members of the public, with nothing to hide and, so, of no interest to these agencies.

There was also recognition that wealthy and weighty, private bodies had the capacity to obtain and apply the most developed technologies and this appeared to arouse greater mistrust: as they were considered to be less subject to the levels of scrutiny applied to public sector agencies. There did seem to be a general lack of awareness, amongst all participants, regarding the actual extent of data matching and mining currently practised across organisations.

Participants believed that the targeted use of smart surveillance and massively integrated dataveillance was a good thing if performed effectively for the statutory reasons of national security, law enforcement *et al*. However, the potential for function creep and errors was recognised and, therefore, the acceptability of this surveillance was conditional upon that legal purpose; and the necessary and effective application of measures to individuals or groups warranting them. They voiced concerns over the expansion of such measures as part of the crime scenarios read out to the group, protesting at the proposed widespread use of tagging and other technologies. As one participant put it: "*If you take this, 'if you have nothing to hide' then people wouldn't have curtains. It doesn't apply to privacy as I understand it"* (P7-II).

5.4.1 Beliefs about democracy and data security

Although there were hints, from some, of an optimistic faith in legal safeguards and an institutional duty to ensure democratic processes in relation to privacy and personal data protection, this was, by no means, a general or majority view. Most participants believed that the situation was far darker: with data being exchanged and/or sold on; consent not being taken seriously or sincerely; legal safeguards evaded or bypassed; and regulatory principles being dwarfed by financial and commercial interests. This was illustrated by participants in the following ways. In relation to consent: "*You should have to sign to say you can do that rather than the various and nefarious ways that they skim round that is unacceptable"* (P6-II). In relation to financial interests, "*there's like the DVLA selling your car details for, I don't know how much, to credit companies and the lines are non-existent with companies getting the data that they want*" (P1-II). Participants believed this to be an unacceptable position: but expressed powerlessness in the face of larger pressures and interests being brought to bear.

There did not appear to be a widely held belief that the state would protect their individual control over their own personal data or the wider democratic process. As one participant described it:

> "*The Government writes the legislation but then loopholes are found in it, so you might think that you've got a right but essentially there may be aspects of your rights which are being invaded due to loopholes*" (P3-II).

As already stated in an earlier section, participants believed that they themselves had succumbed to a degree of privacy trade-off, in which they enjoyed greater convenience in the delivery of goods and services. However, this was not approval for the excesses they perceived in relation to the function creep and data exchange occurring between agencies and between public and private sectors. Although some participants felt that, in the UK, the level of democratic process was higher than in other states, the danger of misuse and abuse, which could arise with future regime change, was also acknowledged.

It was recognised that, within law enforcement fields, surveillance helped greatly with detection and prosecution, but less so with prevention. One participant identified just how persuasive data from surveillance technologies could be within the Criminal Justice System, even if that conviction was not as well justified as it was argued:

> "*My wife's a barrister and she says if you're in a case as soon as there's forensic evidence you can talk about everything else but the jury's not listening after that and barristers use that as part of their game in court. Even if it's tenuous, they'll focus on that and keep emphasising it to the jury over and over again"* (P1-II).

This clearly illustrates how surveillance technology can serve to erode the quality of democratic processes within particular jurisdictions.

6. Conclusion

The three focus groups reaped results that clearly point to significant areas of negativity in the attitudes of citizens - of all ages and genders - in relation to surveillance in general and SMART technologies in particular.

Participants displayed a comprehensive knowledge of the technologies applied across the different spaces they entered as consumers, workers, travellers or recreationally. However, they displayed little knowledge of legal or regulatory provisions for privacy and data protection.

Even when the issue of legal provisions was discussed, participants expressed at least scepticism - if not cynicism - at the law's effectiveness in the prevention of the misuse of data. It was felt that the legal safeguards could be - and were - circumvented by powerful interests.

Differences emerged between the genders and age groups in their views relating to surveillance issues - notably, on safety and privacy issues - and these nuanced and context-dependent features are worthy of more detailed, systematic and empirical exploration. This approach should also be applied to take account of other personal differences - such as, race; religion; health conditions; place of residence; and socio-economic status - as these were beyond the remit of this analysis.

Participants clearly recognised that smart surveillance measures were more powerful and focused than open systems and, as such, were more intrusive and targeted to individuals. This, they felt, was linked to greater potential for misuse and errors with direct consequences for individuals and groups. Therefore, acceptance of the use of such surveillance measures was by no means unconditional.

Participants supported the statutory uses of surveillance - for national and border security, law enforcement and crowd control and for legitimate administrative purposes - and for improving the delivery of goods and services. However, they expected these uses to be bound by a commitment to the principles of consent, necessity and proportionality; and not applied arbitrarily, without permission, or for political and financial interests that lay beyond the primary sphere for which consent was given.

Acknowledgements

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

APPENDIX A – RECRUITMENT QUESTIONNAIRE

Section A

(A1) Gender

- ☐ Male
- ☐ Female

(A2) Age

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45+

(A3) Would you say you live in a

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

(A4) What is your highest level of education?

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

(A5) What is your occupation?

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

Section B

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

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

- ☐ Yes
- ☐ No

(B4) Do you drive a vehicle?

- ☐ Yes
- ☐ No

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

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

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

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

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

- ☐ Yes
- ☐ No

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

- ☐ **Yes**
- ☐ **No**

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

- ☐ Yes
- ☐ No

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

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

APPENDIX B

DISCUSSION GUIDELINES (ENGLISH)

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

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

Objectives	Discussion items and exercises
Word association exercise **[About 5mins]** - *Word-association game serving as an ice-breaker* - *Establish top of mind associations with the key themes* - *Start off the group*	***Item 1*** **First up, we will carry out a short game: I will read out a word and I would like you to say the first couple of things that come to mind when you hear the word. Let's try an example first: What is the first thing that comes to mind if I say the word "*food*"? Preferably, try to think about single words or short phrases, avoiding lengthy descriptions.** *Read Out (one at a time):* *Technology, privacy, national security, personal information, personal*

discussion	*safety* ***Running Total: 15min***
Discussion on everyday experiences related to surveillance **[20min]** *- To explore participants' experience with surveillance & how they perceive it* *- To explore participants' awareness and knowledge of the different surveillance technologies*	***Item 2*** **Let's talk about something else. I want you to think about instances during which you feel that either you or your actions are being observed as well as any instances during which you are aware that information about you is being collected. Let's start by thinking about activities you would usually undertake in your everyday life. Let us take the following situations as examples of this.** **Scenario 1: Supermarket** ***As a first example we can take a shopping trip at your usual supermarket. Can you share your thoughts on this?*** **Scenario 2: Travelling** ***Let's move on to another situation, this time related to travelling. What about when you travel by air?*** **Scenario 3: Public place (e.g. museum, stadium)** ***Now imagine that you are visiting a public place, such as a museum or attending an event such as a sports match or a concert. What kind of activities do you think would be recorded?*** **Scenario 4: Mobile devices** **Let us discuss just one final example. Think about the times you use your mobile phone. What do you think is being recorded in this case?**
Aims: *1. Explore the participants' awareness and knowledge of the technologies* *2. Explore the participants' experience of being monitored in their many roles*	*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. Explore the participants' understanding of where their information is ending up	***3. <u>Who</u> is collecting the information:*** ***a. Who do you think is responsible for collecting and recording your personal information?*** ***b. Where do you think your personal information will end up?***
4. Explore the particiants' views on why their actions and behaviours are observed, monitored and collected	***4. <u>Why</u> the information is being recorded, collected and stored:*** ***a. Why do you think your personal information is being recorded and collected?*** ***b. In what ways do you think your personal information will be used?*** ***Running Total: 35min***
Presentation of cards depicting different technologies and applications [10mins] *To expose participants to a selection of relevant SMART technologies & applications in order to enable a better understanding and hence to facilitate the 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*	***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*

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

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*

Aims:

1. Security climate

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":

1a. What makes you feel safe in the scenario provided?

1b. What makes you feel vulnerable in the scenario provided?

and level of threat

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

2. Deployment of specific technologies

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

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

3. Locations of deployment such as:
Airports
Malls
Streets

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

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

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

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

5. Length of storage of surveillance data

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

To help you probe, provide the following examples to the participants:
- ***Recordings of CCTV***
- ***The location and movement of cars***
- ***The storage of DNA, fingerprints and iris scans***
- ***The location of citizens who pose a risk to others***
- ***The location and movements of elderly people and children***

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

Running Total: 1 hour 35min

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

APPENDIX C – 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 D – CONSENT FORM

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

Participation

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

Confidentiality and anonymity

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

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

Data protection and data security

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

Risks and benefits

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

Questions about the research

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

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

Signature: Date:

APPENDIX E – CODING MAP

1. Surveillance technologies in different spaces

1.1. Spaces
- 1.1.1. Transport
- 1.1.2. Retail
- 1.1.3. Entertainment
- 1.1.4. Mobile communications

1.2. Awareness of different surveillance methods/technologies
- 1.2.1. Drones
- 1.2.2. GPS
- 1.2.3. Key stroke logging

1.3. Perceived purposes
- 1.3.1. National and border security
- 1.3.2. Law enforcement and crowd control
- 1.3.3. Commercial and financial purposes
- 1.3.4. Administrative purposes
- 1.3.5. Logistical purposes
- 1.3.6. Create data pools
- 1.3.7. Data vending

1.4. Acceptance
- 1.4.1. Convenience
  - 1.4.1.1. Ease and availability of goods and services
- 1.4.2. Loss of privacy and control over data
- 1.4.3. Vulnerability and mistrust

2. Perceptions and attitudes towards smart surveillance and integrated dataveillance

2.1. Negative feelings
- 2.1.1. Lack of confidence
- 2.1.2. Fear and mistrust
- 2.1.3. Powerlessness and frustration
- 2.1.4. Indignation and anger
- 2.1.5. Conflict
- 2.1.6. Beliefs
  - 2.1.6.1. Blurring of boundaries
  - 2.1.6.2. Consent
  - 2.1.6.3. Abuse of data
  - 2.1.6.4. Financial and commercial interests
  - 2.1.6.5. Potential for errors
  - 2.1.6.6. Legal compliance
  - 2.1.6.7. Political interests

2.1.6.8. Intrusiveness

2.2. Personal differences in negative feelings

2.2.1. Age and gender differences

2.3. Positive feelings

2.3.1. Convenience

2.3.1.1. Provision of goods and services

2.3.1.2. Enhanced health and safety

2.3.2. Potential for misuse

2.4. Personal differences in positive feelings

2.4.1. Gender differences

3. Behaviours and intentions

3.1.1. Active intention

3.1.1.1. Complaint to the organisation

3.1.2. Passive reactions

3.1.2.1. Consent without protest

4. Beliefs about current and future smart surveillance and massively integrated dataveillance

4.1. Beliefs about democracy and data security

4.1.1. Financial and commercial interests

4.1.2. Loopholes in the legislation

4.1.3. Privacy-convenience trade-off

4.1.4. Efficiency of surveillance in crime prevention and prosecution