RESPECT

Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies

The citizens' perspective: Awareness, feelings and acceptance of surveillance and surveillance systems for fighting crime in Austria. A quantitative study.

Noellie Brockdorff[1], Sandra Appleby-Arnold[1], Janos Böszörmenyi[2]
[1]Department of Cognitive Science, University of Malta, Msida, Malta
[2]University of Vienna, Austria

May 2015

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

RESPECT
Rules, Expectations & Security through privacy-enhanced convenient technologies (G.A. 285582).
The project was co-financed by the European Union within the Seventh Framework Programme (2007-2013).
http://www.respectproject.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

0. Executive Summary

This document presents the results for Austria within the framework of a larger study undertaken as part of the RESPECT project. Analyses are based on a survey regarding the perceptions, feelings, attitudes and behaviours of citizens towards surveillance for the purpose of fighting crime, carried out amongst a quota sample that is representative of the population in Austria for age (citizens aged between 18 and 64[1]) and gender, based on Eurostat data of 12/2012. Responses were gathered, predominantly, through an online survey supplemented by a number of questionnaires administered in face to face interviews, in order to fulfil the quota and also reach those citizens who do not use the internet. The questionnaire consisted of 50 questions and was available online in all languages of the European Union between November 2013 and March 2014. The face to face interviews were carried out between January and March 2014. The Austrian sample is based on the responses from 135 individuals who indicated Austria as their country of residence in the online survey or were administered the questionnaire face to face.[2]

Generally, the data reveal a rather large spread in the Austrian respondents' knowledge of different types of surveillance and surveillance technologies, with CCTV (99%) being the type most respondents have heard of and the surveillance of "suspicious" behaviour (50%) the least known. Most respondents also indicated that they know of a number of reasons for the setting up of surveillance, ranging between 95% for the prosecution of crime and 77% for the control of crowds. Most respondents think that surveillance is taking place in the country where they live, but more than half of the respondents felt that they do not know about the economic costs of surveillance.

The perceived usefulness of the different types of surveillance investigated in this study depends on the respective purpose: Surveillance of financial transactions is perceived to be the most useful for reduction of crime, CCTV cameras are perceived to be the most useful for detection of crime, and geolocation surveillance is perceived to be the most useful for prosecution of crime. Surveillance of online social networking and surveillance using databases containing personal information were perceived to be the least useful. The highest mean score[3] was achieved for geolocation surveillance for the purpose of prosecution of crime (3.58) and the lowest for surveillance of online social networking for the purpose of reduction of crime (2.03). Generally, surveillance was perceived as being most useful for the prosecution of crime and least useful for the reduction of crime. The results for perceived effectiveness of the different types of surveillance in protecting against crime follow the same pattern of results as for perceived usefulness of the same types of surveillance. However, the different types of surveillance are perceived as less effective in the protection against crime than they are deemed useful for the reduction, detection, and prosecution of crime, and different acceptance levels in different locations point at acceptance of surveillance rather being related to respondents having become accustomed to surveillance in city centres and urban areas.

The presence of surveillance appears to make only a small minority of Austrian respondents feel secure (9%); more than half of the respondents feel insecure when surveillance is present. Regarding the respondents' feelings about personal information gathered through surveillance, respondents feel generally a very strong lack of control over processing of personal information gathered via surveillance, irrespective of whether it has been gathered by

[1] The number of respondents aged 65 and older (15 respondents) was not sufficient to be representative for this segment of the Austrian population. Therefore, it was decided to remove these responses and recalculate the sample requirements for all other age groups in order to achieve a sample that is representative for the Austrian population aged between 18 and 64.

[2] The overall Austrian sample consists of 260 respondents. However, due to the fact that most responses were collected through an online survey, in some of the age/gender subgroups more responses were collected than were needed to complete the quota. In such cases, the questionnaires to be used were randomly selected from amongst the responses collected for that subgroup.

[3] On a scale from 1 to 5, with 1=not useful at all, and 5=very useful.

government agencies or by private companies. Additionally, there is a visible lack of trust in both private companies and government agencies being able to protect personal information gathered via surveillance, with more mistrust towards private companies than towards government agencies. Consequently, there may not only be a missing link between surveillance and feelings of security, but also perceptions of a substantial lack of data protection in connection with personal information gathered through surveillance.

The majority of respondents feel more unhappy than happy with all the different types of surveillance investigated, and they also feel more unhappy than happy about surveillance taking place without people knowing about it.

Most Austrian respondents agreed more than disagreed that all types of surveillance investigated have a negative impact on their privacy. The strongest negative impact on privacy was perceived for surveillance using databases containing personal information. Moreover, only very few respondents (3-4%) are willing to accept financial compensation in exchange for surveillance measures that would involve greater invasion of privacy.

The sharing of information gathered through surveillance by government agencies with other government agencies, or with foreign governments, is deemed acceptable by the majority of respondents if the citizen is suspected of wrong-doing. However, most of these respondents believe it is necessary that the surveillance needs to be legally authorised for it to be acceptable, and sharing information with private companies is much less acceptable even if surveillance has been lawfully authorised. An even lower number of respondents find it fully acceptable, or acceptable even if the citizen is suspected of wrong-doing, for private companies to share a citizen's personal information. Generally, there is a considerable number of respondents who feel that, unless information or consent has been given, private information should "stay private".

Only a minority of Austrian respondents agreed that surveillance may hold social benefits such as the protection of the individual or protection of the community, but risks ("social costs") associated with surveillance seemed to be more keenly felt. The highest risks were perceived to be privacy invasion (mean score 6.75[4]), misinterpretation (6.63) and intentional misuse of information (6.57) arising from surveillance, followed by loss of control over the usage of one's personal data gathered via surveillance. Discrimination, stigma, and the limitation of citizen rights as consequences of surveillance appear also to be of major concern. This concern about the disadvantages of surveillance may be the reason that respondents reported some changes in personal behaviour as a consequence of awareness of surveillance. About two thirds of the respondents have stopped accepting discounts in exchange for personal data (66%[5]) or have kept themselves informed about technical possibilities to protect their personal data (63%), and a substantial minority have restricted their activities or the way they behave (46%[3]), or avoided locations or activities that they suspect are under surveillance (30%[3]).

There were some significant gender differences in the findings. Female respondents had heard less of the surveillance of "suspicious" behaviour or surveillance of financial information, and they were less aware of whether surveillance of financial transactions or surveillance using databases containing personal information is taking place in the country where they live. Female respondents also perceived CCTV cameras (for the reduction of crime) and geolocation surveillance (for the detection of crime) significantly more useful than male respondents, but there were no differences between male and female responses regarding the perceived effectiveness of the different surveillance measures investigated. There were also no gender differences in feelings of security (or insecurity) due to the presence of surveillance, feelings of control over one's personal information gathered via surveillance measures, trust that personal information gathered by government agencies and private companies via surveillance

[4] On a scale from 1 to 7, with 1=disagree, and 7=agree.
[5] Answers 5, 6 or 7 on a scale from 1 to 7, with 1=disagree and 7=agree.

measures is protected, perceptions of privacy, and feelings of general happiness with surveillance measures. Female respondents reported less behavioural changes resulting from surveillance than males; in particular, female respondents indicated less often that they had taken defensive measures, and that they had kept themselves informed about technical possibilities to protect their personal data.

To summarise, the Austrian respondents felt more insecure than secure in the presence of surveillance, and they indicated a strongly felt lack of trust in the protection of, and control over, personal information gathered via surveillance. A majority also feel more unhappy than happy with the different types of surveillance. Additionally, there is a link between feeling happy, or unhappy, about surveillance and feeling secure or insecure through the presence of surveillance. However, analyses also indicate that increasing the perceived effectiveness of surveillance measures and, in particular, increasing the perceived effectiveness of laws regarding the protection of personal data gathered via surveillance may make citizens feel more secure.

Further research is needed to disentangle the relationships between surveillance measures, feelings of security or insecurity, and citizens' general quality of life feelings.

1. Introduction

The analyses and results in this document are based on a survey regarding the perceptions, feelings, attitudes and behaviour of European citizens towards surveillance for the purpose of fighting crime. This study was undertaken as part of the RESPECT project – "Rules, Expectations and Security through Privacy-enhanced Convenient Technologies" (RESPECT; G.A. 285582) – which was co-financed by the European Commission within the Seventh Framework Programme (2007-2013). Quota samples were used for each RESPECT partner country which were based on demographic data retrieved from the Eurostat statistics of December 2012.[6] Responses were gathered, predominantly, through an online survey supplemented by a number of questionnaires administered in face to face interviews, in order to fulfil quotas and reach those citizens who do not use the internet. The survey consisted of 50 questions and sub-questions, and was available online in all languages of the European Union from November 2013 until March 2014.[7] A snowball technique was used to promote the study and disseminate links to the questionnaire. Most RESPECT partners placed advertisements on their respective university/institute website and those of related institutions, sent out press releases and placed banners or advert links in local online newspapers or magazines, posted links to the questionnaire on social networking websites, sent the link out in circular emails (e.g., to university staff and students), and used personal and professional contacts to promote the survey. In order to achieve the quota a number of questionnaires were administered in face to face interviews. Typically, these face to face interviews were required for the older age groups as internet usage is not as common amongst older citizens as it is with the younger population.

Overall, 5,361 respondents from 28 countries completed the questionnaire. This total sample shows a very even gender and age distribution, which is unsurprising given that target quotas were set for each RESPECT partner country. The Austrian sample used for this analysis is based on the responses from 135 individuals who indicated Austria as their country of residence in the online survey or were administered the questionnaire face to face. The sample has a gender distribution of 49.6% females and 50.4% males, and an age distribution that is representative for Austrian citizens between 18 and 64 years (see figure 1 below).

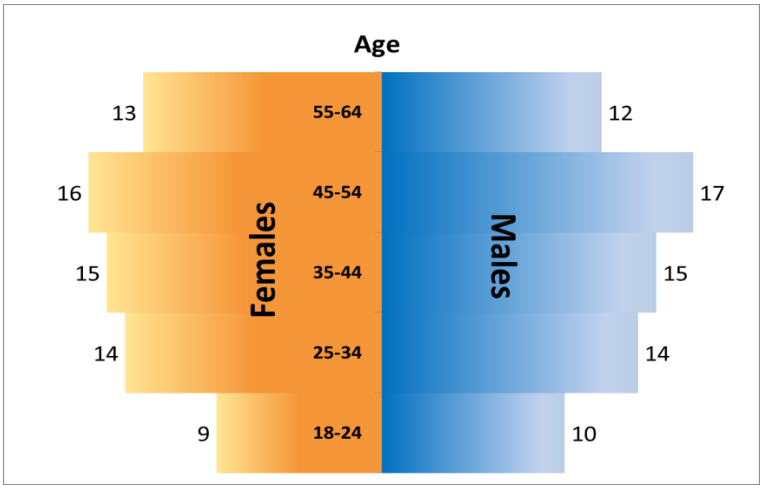

Figure 1: Age and gender distribution of Austrian quota sample

Not fully satisfactory is the high level of education of the majority of respondents (76% with tertiary or post-graduate education). However, this was to be expected due to the majority of responses being collected online as well as several of the recruiting institutions being academic entities, and it coincides with the education level of

[6] Source: http://epp.eurostat.ec.europa.eu/portal/page/portal/population/data/main_tables.
[7] The English version of this this questionnaire may be seen in Appendix B.

respondents in the total RESPECT sample (73%). Regarding specific demographic data related to aspects of surveillance, 12% of Austrian respondents (16% of total sample) felt that they were living in an area with increased security risks, 76% (53% total sample) indicated that they usually travel abroad at least twice per year, and 79% (71% total sample) responded that they usually visited a mass event at least twice per year. Therefore, it can be assumed that the majority of respondents are frequently exposed to a variety of surveillance measures that are intended to fight crime.

This report presents results on citizens' perceptions, awareness, acceptance of, and feelings towards, surveillance, and the potential relationships between these factors. Furthermore, separate analyses are dedicated to the social and economic costs of surveillance – covering also the additional aspect of behaviour and behavioural intentions – which are specific tasks within the RESPECT project. Whereas age-related aspects could not be analysed due to the rather low number of respondents per age group, gender aspects are discussed throughout all sections alongside the general results.

2. Citizens' knowledge of surveillance

2.1 Awareness of different types of surveillance

Generally, there can be observed a rather large spread in the awareness of different types and technologies of surveillance. Almost all Austrian respondents (98.5%) indicated that they have heard of CCTV, whereas just about half (50.4%) had heard of the surveillance of "suspicious" behaviour. The only two statistically significant differences between female and male responses are male respondents indicating a greater awareness of "suspicious" behaviour (difference of 23 percentage points), and having heard more of financial tracking as a surveillance measure (difference of 10.5 percentage points).

Table 1
Knowledge of types of surveillance

		Answer = YES		
		Total	**Female**	**Male**
Q1_1	**Biometric data**, e.g. analysis of fingerprints, palm prints, facial or body features	91.9%	91.0%	92.6%
Q1_2	**"Suspicious" behaviour**, e.g. automated detection of raised voices, facial or body features	50.4%	38.8%	61.8%*
Q1_3	**Data and traffic on the internet**, e.g. Deep Packet/Content inspection	88.9%	88.1%	89.7%
Q1_4	**Databases** containing personal information, e.g. searching state pension databases, or customer databases of private companies	88.1%	83.6%	92.6%
Q1_5	**Online communication**, e.g. social network analysis, monitoring of chat rooms or forums	96.3%	95.5%	97.1%
Q1_6	**Telecommunication**, e.g. monitoring of phone calls or SMS	97.8%	97.0%	98.5%
Q1_7	**Electronic tagging / Radio Frequency Identification** (RFID), e.g. tracking geolocation with electronic chips implanted under the skin or in bracelets	91.1%	89.6%	92.6%
Q1_8	**Global Positioning Systems** (GPS), e.g. tracking geolocation of cars or mobile phones	97.0%	97.0%	97.1%
Q1_9	**CCTV cameras**, e.g. in public places, airports or supermarkets	98.5%	98.5%	98.5%
Q1_10	**Financial information**, e.g. tracking of debit/credit card transactions	91.9%	86.6%	97.1%*

Q1: Have you ever heard of the use of any of the below for the purpose of monitoring, observing or tracking of people's behaviour, activities or personal information?
Note: Results in this table marked with an asterisk (*) signify that the results between males and females are statistically significantly different (p<.05). Other differences between males and females are not statistically significant.

2.2 Known reasons for surveillance

Most respondents are aware of the main reasons for deploying surveillance. The reason for surveillance that is most known about is the prosecution of crime (94.8%), and the least known is the use of surveillance for control of crowds (77%). There are no statistically significant gender differences in knowing of the reasons for surveillance specifically asked for.

Table 2
Known reasons for surveillance

		Answer=YES		
		Total	**Female**	**Male**
Q2_1	The reduction of crime	83.7%	83.6%	83.8%
Q2_2	The detection of crime	88.9%	88.1%	89.7%
Q2_3	The prosecution of crime	94.8%	95.5%	94.1%
Q2_4	Control of border-crossings	88.1%	83.6%	92.6%
Q2_5	Control of crowds	77.0%	74.6%	79.4%
Q2_6	Other	32.6%	29.9%	35.3%
Q2_7	I don't know of any reasons.	0.7%	0.0%	1.5%

Q2: What reasons for the setting up of surveillance do you know of?
Note: Results in this table marked with an asterisk (*) signify that the results between males and females are statistically significantly different (p<.05). Other differences between males and females are not statistically significant.

3. Perceived usefulness and effectiveness of surveillance

3.1 Perceived usefulness

Which type of surveillance is perceived to be more useful than the others depends on the respective purpose. For the reduction of crime, surveillance of financial transactions was perceived the most useful; for the prosecution of crime, respondents found CCTV cameras to be the most useful; and for the prosecution of crime it was geolocation surveillance that was perceived to be the most useful. Generally, the different types of surveillance were perceived to be most useful for the prosecution of crime, slightly less useful for the detection of crime, and less useful still for the reduction of crime[8]. However, only the surveillance of financial transactions and CCTV surveillance are perceived to be useful for all three purposes[9]. Geolocation surveillance was perceived to be useful only for the prosecution of crime, surveillance using databases containing personal information and surveillance of online social networking were not perceived to be useful for any of the three purposes investigated.

There were, again, very few significant gender differences in the perception of usefulness of surveillance. CCTV cameras for the purpose of reduction of crime and geolocation surveillance for the detection of crime were perceived to be more useful by female than by male respondents.

[8] With the exception of CCTV cameras which were perceived most useful for the detection of crime, slightly less useful for the prosecution of crime, and least useful for the reduction of crime.
[9] Mean result in all categories above the midpoint of 3.00 in Table 3.

Table 3

Perceived usefulness of surveillance

		Total		Female		Male	
Q3.1	**the reduction of crime**	**Mean**	**STD**	**Mean**	**STD**	**Mean**	**STD**
Q3.1_1	CCTV cameras	3.11	1.341	3.40	1.311	2.83*	1.318
Q3.1_2	Surveillance using databases containing personal information	2.28	1.300	2.44	1.376	2.14	1.223
Q3.1_3	Surveillance of online social networking	2.03	1.092	2.03	1.066	2.03	1.123
Q3.1_4	Surveillance of financial transactions	3.20	1.336	3.19	1.224	3.22	1.442
Q3.1_5	Geolocation surveillance	2.61	1.442	2.83	1.391	2.42	1.468
Q3.2	**the detection of crime**						
Q3.2_1	CCTV cameras	3.38	1.374	3.57	1.420	3.20	1.315
Q3.2_2	Surveillance using databases containing personal information	2.40	1.364	2.64	1.542	2.20	1.162
Q3.2_3	Surveillance of online social networking	2.26	1.214	2.34	1.207	2.18	1.223
Q3.2_4	Surveillance of financial transactions	3.21	1.378	3.29	1.373	3.14	1.391
Q3.2_5	Geolocation surveillance	2.69	1.418	3.03	1.505	2.36*	1.260
Q3.3	**the prosecution of crime**						
Q3.3_1	CCTV cameras	3.34	1.367	3.47	1.327	3.23	1.401
Q3.3_2	Surveillance using databases containing personal information	2.89	1.332	3.09	1.391	2.71	1.263
Q3.3_3	Surveillance of online social networking	2.62	1.331	2.66	1.352	2.58	1.322
Q3.3_4	Surveillance of financial transactions	3.53	1.272	3.50	1.218	3.56	1.326
Q3.3_5	Geolocation surveillance	3.58	1.350	3.68	1.319	3.49	1.382

_____

Q3: How useful in general do you think the following types of surveillance are for […] (1=not useful at all; 5=very useful)
Note: Results in this table marked with an asterisk (*) signify that the results between males and females are statistically significantly different (p<.05). Other differences between males and females are not statistically significant.

The potential relationships between the perceived usefulness of different types of surveillance for the reduction, detection and prosecution of crime were examined (See Table A1 in Appendix A). It appears that there is a relationship between beliefs about the usefulness of the various types of surveillance for different purposes. For example, if a respondent perceives surveillance of online social networking as useful for the reduction of crime then the respondent is also likely to perceive this form of surveillance as useful for the detection of crime and prosecution of crime. There is a similar pattern of responses for all types of surveillance, with the relationship between perceived usefulness for reduction of crime and perceived usefulness for detection of crime typically being the strongest, followed by the relationship between detection of crime and prosecution of crime. This pattern of responses suggests that the concepts of reduction, detection, and prosecution of crime may be somewhat entangled. However, it is also possible that some respondents decided on a general "usefulness setting" for each type of technology and answered the questions on the reduction, detection, and prosecution of crime in the same way. The overall closest relationships were found for surveillance of online social networking sites and surveillance using databases containing personal information between their respective usefulness for reduction and their usefulness for detection of crime. Furthermore, strong relationships are observed between the perceived usefulness of surveillance using databases containing personal information for the reduction of crime and the perceived usefulness of surveillance of social networking sites for the same purpose. Another strong relationship is present between the perceived usefulness of surveillance using databases containing personal information for the detection of crime and geolocation surveillance for the same purpose. Similar relationships between these types of surveillance can be found for the other two purposes respectively. This may, again, be the result of some

respondents not distinguishing much between the different types of surveillance and rather focusing on the usefulness of surveillance generally for different purposes.

There is no correlation between the knowledge of general purposes of surveillance, and the assumed usefulness of specific types of surveillance for these purposes. A reason for this missing link may be that surveillance still represents a somewhat abstract concept for the majority of citizens. To imagine specific purposes, these need to be linked to specific types, technologies or measures of surveillance.

3.2 Effectiveness in protection against crime

The results for perceived effectiveness of the different types of surveillance in protecting against crime follow the same pattern of results as for perceived usefulness of the same types of surveillance in the reduction, detection, and prosecution of crime. However, the different types of surveillance are generally perceived to be less effective in protection against crime than they are deemed to be useful for the reduction, detection, and prosecution of crime, and for all types of surveillance the majority of respondents disagreed rather than agreed that they are an effective way to protect against crime[10]. Comparing perceived usefulness with perceived effectiveness of types of surveillance, for example between 37%[11] (reduction of crime) and 47%[12] (prosecution of crime) of respondents believed that surveillance of financial transactions is useful, but only 36%[13] of respondents agreed that it is effective, and whereas between 36% and 47% of respondents believed that CCTV is a useful type of surveillance, only 33% deemed it to be effective. Surveillance of financial transactions is perceived to be the most effective (or, rather, least ineffective) surveillance measure in protection against crime, followed by CCTV and geolocation surveillance. Surveillance of online social-networking and surveillance using databases containing personal information are seen to be the least effective methods of protection against crime.

Table 4

Perceived effectiveness of surveillance

		Total		Female		Male	
		Mean	STD	Mean	STD	Mean	STD
Q5.1.1_1	CCTV is an effective way to protect against crime	3.64	1.873	3.83	1.865	3.46	1.878
Q5.1.1_2	Surveillance utilising databases containing personal information is an effective way to protect against crime	2.57	1.626	2.64	1.778	2.52	1.501
Q5.1.1_3	Surveillance of online social-networking is an effective way to protect against crime	2.40	1.666	2.30	1.442	2.49	1.854
Q5.1.1_4	Surveillance of financial transactions is an effective way to protect against crime	3.65	2.026	3.59	1.909	3.70	2.139
Q5.1.1_5	Geolocation surveillance is an effective way to protect against crime.	3.09	1.884	3.25	1.917	2.94	1.855

Q5.1.1: How much do you agree or disagree with the following statements […] (1=disagree; 7=agree)

Note: Results in this table marked with an asterisk (*) signify that the results between males and females are statistically significantly different (p<.05). Other differences between males and females are not statistically significant.

[10] Results for all types of surveillance were below the midpoint of 4.0.

[11] Answers 4 or 5 on a scale from 1 to 5, with 1=not useful at all and 5=very useful.

[12] Answers 4 or 5 on a scale from 1 to 5, with 1=not useful at all and 5=very useful.

[13] Answers 5, 6 or 7 on a scale from 1 to 7, with 1=disagree and 7=agree.

3.3 Relationship between perceived usefulness and effectiveness

There is a clear relationship between the perceived usefulness of a type of surveillance in the reduction, detection, and prosecution of crime and the perceived effectiveness of that type of surveillance in the protection against crime (see Table A8 in Appendix A). The strongest relationship for most types of surveillance is found between perceived usefulness in detection of crime and perceived effectiveness in the protection against crime. This was the case for surveillance using databases containing personal information, surveillance of online social networking and surveillance of financial transactions. In the case of CCTV and geolocation surveillance, the perceived effectiveness of these modes of surveillance as a means to protect against crime was related most closely with their perceived usefulness in reduction of crime. However, it has to be kept in mind that these relationships do not only link perceived usefulness and perceived effectiveness, but also their negative side – a perceived lack of usefulness and, correspondingly, a perceived lack of effectiveness.

4. Perceptions of surveillance

4.1 Surveillance and feelings of security

As seen in the previous section, only some of the different types of surveillance are perceived as useful in the reduction, detection, and prosecution of crime and, at an even lower level, effective in the protection against crime. Similarly, surveillance does not produce the feelings of security that may be expected (see Table 5 in next section). Only 9% of respondents feel secure in the presence of surveillance (4 or 5 on a 5-point scale, with 1=very insecure and 5=very secure). But more than half of the respondents (57%) feel insecure (1 or 2 on a 5-point scale, with 1=very insecure and 5=very secure) when surveillance is present. The remaining respondents indicated either the mid-point of the scale (26%), or "I don't know" (8%).

4.2 Personal information collected through surveillance

Respondents generally feel a very strong lack of control over the processing of personal information gathered via surveillance, irrespective of whether it has been gathered by government agencies or by private companies. There is also a visible lack of trust in both private companies and government agencies being able to protect personal information gathered via surveillance, but with more mistrust towards private companies than towards government agencies. Consequently, there may not only be a missing link between surveillance and security, but also perceptions of a substantial lack of data protection in connection with personal information gathered through surveillance. No statistically significant gender differences could be found in the feelings of trust into government agencies or private companies and control over personal data collected by them.

Table 5
Feelings of security, control and trust

		Total		Female		Male	
4.3	**Security** (1=very insecure; 5=very secure)	**Mean**	**STD**	**Mean**	**STD**	**Mean**	**STD**
	How secure does the presence of surveillance measures make you feel	2.25	0.993	2.26	0.929	2.24	1.058
4.4	**Control** (1= no control; 5=full control)						
4.4.1	How much control do you think you have over the processing of personal information gathered by government agencies via surveillance measures?	1.62	0.988	1.44	0.819	1.78	1.104

4.4.2	How much control do you think you have over the processing of personal information gathered by private companies via surveillance measures?	1.54	0.803	1.43	0.749	1.65	0.842
4.5	**Trust** (1=no trust; 5=complete trust)						
4.5.1	How much do you trust government agencies that they protect your personal information gathered via surveillance measures?	2.07	1.101	2.09	1.092	2.06	1.118
4.5.2	How much do you trust private companies that they protect your personal information gathered via surveillance measures?	1.43	0.719	1.39	0.742	1.46	0.700

Note: Results in this table marked with an asterisk (*) signify that the results between males and females are statistically significantly different (p<.05). Other differences between males and females are not statistically significant.

4.3 "Happiness" with surveillance

The majority of respondents feel more unhappy than happy with the different types of surveillance. They appear to feel most unhappy with surveillance using databases containing personal information with a large majority of participants feeling unhappy (67%[14], mean score 4.19). About two thirds of respondents felt unhappy with online social networks and geolocation surveillance and one third felt neither happy nor unhappy. In the case of CCTV and the surveillance of financial transactions, the number of those participants who feel unhappy about those types and surveillance and those participants who felt neither happy nor unhappy is fairly evenly distributed (between 44% and 46% respectively) A majority of respondents is also unhappy with surveillance taking place without people knowing about it. There is no significant difference between female and male responses, except for geolocation surveillance where female respondents felt less unhappy than male respondents.

Table 6
Happiness with surveillance

		Total		Female		Male	
		Mean	**STD**	**Mean**	**STD**	**Mean**	**STD**
5.3_1	Feel happy/unhappy about CCTV cameras	3.56	0.996	3.40	0.997	3.71	0.978
5.3_2	Feel happy/unhappy about surveillance of online social networks	4.09	0.927	4.00	0.905	4.16	0.947
5.3_3	Feel happy/unhappy about surveillance using databases	4.19	0.894	4.15	0.903	4.23	0.891
5.3_4	Feel happy/unhappy about surveillance of financial transactions	3.50	1.109	3.49	1.120	3.51	1.106
5.3_5	Feel happy/unhappy about geolocation surveillance	4.04	0.984	3.85	0.988	4.22*	0.951
5.4	Feel happy/unhappy about surveillance taking place without noticing	4.17	0.955	4.11	0.886	4.22	1.020

Q5.3: How happy do you feel about the following types of surveillance […] (1=very happy; 5=very unhappy)
Q5.4: How happy do you feel about surveillance taking place without being aware of it? (1=very happy; 5=very unhappy)
Note: Results in this table marked with an asterisk (*) signify that the results between males and females are statistically significantly different (p<.05). Other differences between males and females are not statistically significant.

[14] Scores 4 and 5 on a scale from 1=very happy to 5=very unhappy.

4.4 Relationship between security and happiness

There are moderate to strong correlations between citizens' feelings of being happy, or unhappy, with different types of surveillance (see table A9 in Appendix A). For example, respondents who are happy or unhappy with surveillance using databases containing personal information are also likely to be happy or unhappy with social-networking surveillance. And those who are happy or unhappy with geolocation surveillance have the same feelings about CCTV, social-networking surveillance, and surveillance using databases containing personal information. As was the case in Section 3.1 above, this may be the result of several respondents not distinguishing much between the different types of surveillance.

There is also a moderate relationship between generally feeling happy or unhappy about different types of surveillance and being happy or unhappy with surveillance taking place without one's knowledge, in particular for the surveillance of online social networking. Additionally, being happy or unhappy with different types of surveillance is moderately related to feelings of security as a consequence of the presence of surveillance; this relation is most evident for geolocation surveillance, and least for the surveillance of financial transactions. Furthermore, being happy or unhappy with the different types of surveillance is linked to the perceived usefulness of this type of surveillance for the reduction, detection and prosecution of crimes (see table A2 in Appendix A).

4.5 Surveillance and privacy

Table 7
Perceptions of privacy

		Total		Female		Male	
		Mean	STD	Mean	STD	Mean	STD
5.1.2_1	CCTV has a negative impact on one's privacy	4.65	2.067	4.35	2.049	4.96	2.056
5.1.2_2	Surveillance via databases has a negative impact on one's privacy	5.33	2.062	5.34	2.056	5.31	2.083
5.1.2_3	Surveillance of online social networks has a negative impact on one's privacy	5.2	2.178	5.15	2.246	5.26	2.129
5.1.2_4	Surveillance of financial transactions has a negative impact on one's privacy	4.29	2.254	4.29	2.331	4.29	2.196
5.1.2_5	Geolocation surveillance has a negative impact on one's privacy	5.24	2.176	5.35	2.033	5.14	2.318

Q5.1.2: How much do you agree or disagree with the following statements […] (1=disagree; 7=agree)
Note: Results in this table marked with an asterisk (*) signify that the results between males and females are statistically significantly different (p<.05). Other differences between males and females are not statistically significant.

The majority of respondents agreed more than disagreed that all types of surveillance investigated in this study have a negative impact on one's privacy (Table 7). The highest negative impact on privacy was perceived for surveillance using databases containing personal information. Irrespective of their views on the impact of different types of surveillance on privacy, very few respondents, both male and female, are willing to accept financial compensation in exchange for surveillance measures that would involve greater invasion of privacy (Table 8).

Table 8
Financial privacy trade-off

5.1.3	Would you be willing to accept payment as compensation for greater invasion of your privacy, using:	Answer=YES		
		Total	Female	Male
5.1.3_1	Surveillance via CCTV cameras	2.8%	0.0%	5.6%
5.1.3_2	Surveillance of online social networks	2.8%	0.0%	5.6%
5.1.3_3	Surveillance utilising databases containing personal information	2.8%	1.8%	3.7%
5.1.3_4	Surveillance of financial transactions	3.7%	3.6%	3.7%
5.1.3_5	Geolocation surveillance	2.8%	1.8%	3.7%

Note: Results in this table marked with an asterisk (*) signify that the results between males and females are statistically significantly different (p<.05). Other differences between males and females are not statistically significant.

Respondents' feelings of security or insecurity due to the presence of surveillance are moderately related to their perceived impact of surveillance on privacy (see table A10 in Appendix A). Perceived impact of surveillance on privacy was also moderately related with feelings of trust in private companies and government agencies being able to protect personal information gathered via surveillance, whilst there is practically no relation between a perceived impact of surveillance on privacy and feelings of control over processing of personal information gathered via surveillance. Therefore, despite the clearly perceived lack of trust and control in the context of

personal information gathered during surveillance, and a clearly perceived negative impact of surveillance on one's privacy, these feelings appear to be only partially related.

4.6 Relationships between feelings, effectiveness of surveillance measures, and related laws

There are only weak relationships between the respondents feeling secure due to the presence of surveillance, and feelings of control over their personal data collected through surveillance. Only feelings of security due to the presence of surveillance and trust that personal data gathered by government agencies through surveillance is protected show a moderate link. A similar picture is revealed when looking at the relationship between feelings of control over personal information and trust in its protection (see table A11 Appendix A).

The relationship between the perceived effectiveness of data protection laws and feelings of trust that personal data gathered by government agencies through surveillance is protected is stronger than the relationship with feelings of trust that personal data gathered by private companies is protected. This finding may be due to the fact that data protection laws are perceived as being applied by or being applicable to government agencies more than to private companies. There is a strong relationship between the perceived effectiveness of laws regarding the protection of personal information gathered via surveillance measures and feelings of security produced by surveillance. It is unclear what the basis of such a relationship may be, but it would appear that an increased belief in the effectiveness of data protection laws may produce an increased feeling of security in the presence of surveillance, whilst the respondents' current feelings of insecurity are linked to a perceived low effectiveness of laws[15].

There is also a relationship between perceived effectiveness of different surveillance measures and feelings of security in the presence of surveillance (see table A12 Appendix A), but it is, with the exception of surveillance of social networking, only a moderate one. This suggests that increasing the perceived effectiveness of data protection laws related to surveillance may, to a certain extent, increase citizens' feelings of security in the presence of surveillance more than increasing the effectiveness of such measures themselves.

[15] Mean score 2.49 on a scale from 1 to 5, with 1=not effective at all and 5=very effective).

5. Awareness of surveillance taking place

5.1 Noticing CCTV

Table 9

Whether CCTV is noticed

Q5.2.1	Total	Female	Male
I never notice CCTV cameras.	0.7%	1.5%	0.0%
I rarely notice CCTV cameras.	11.9%	13.4%	10.3%
I sometimes notice CCTV cameras.	37.8%	41.8%	33.8%
I often notice CCTV cameras.	42.2%	34.3%	50.0%
I always notice CCTV cameras.	7.4%	9.0%	5.9%
I don't know / No answer	0.0%	0.0%	0.0%

Q5.2.1: Which of the following best describes you? […]
Note: Results in this table marked with an asterisk (*) signify that the results between males and females are statistically significantly different (p<.05). Other differences between males and females are not statistically significant.

There are no gender differences in whether CCTV is noticed. Overall, about half of the respondents (49.6%) often or always notice CCTV cameras, but only 12.6% of respondents rarely or never notice CCTV cameras.

5.2 Beliefs about surveillance taking place

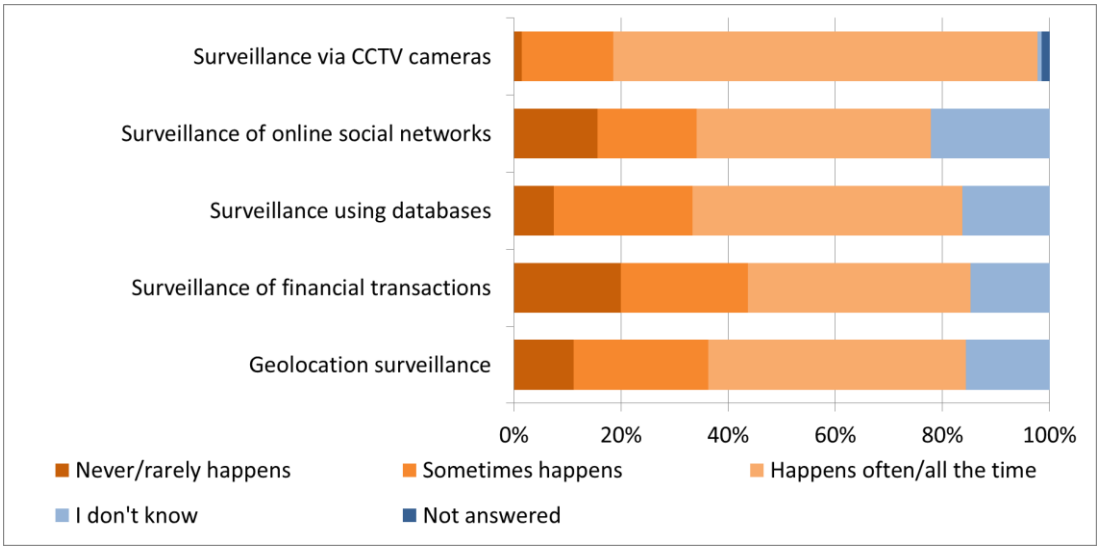

Figure2: Q5.2.2 – In your opinion, how often do the following types of surveillance take place in the country where you live?

Not very surprisingly, a large majority of respondents believes that CCTV surveillance takes place often or all the time in the country where they live (79.3%). Far fewer respondents believe that the other types of surveillance take place, between 42% and 50% for surveillance of online social-networking, surveillance using databases containing personal information, surveillance of financial transactions and geolocation surveillance. However, there is a considerable proportion of respondents who indicated for these types of surveillance that they, actually, "don't know" whether or how often such surveillance takes place in their country (15-22%). A significant gender difference can be found in the answer "I don't know" where the "gap" is up to 18 percentage points between male and female responses (i.e., female respondents more often indicating "I don't know" than male respondents).

6. Acceptability of data sharing practices

Table 10

Acceptability of data sharing practices of government agencies

	Sharing citizens' information gathered via surveillance measures with other government agencies	Sharing citizens' information gathered via surveillance measures with foreign governments	Sharing citizens' information gathered via surveillance measures with private companies
Fully acceptable in all circumstances	2.2%	3.0%	8.9%
Acceptable only if the citizen is suspected of wrong-doing	19.3%	16.3%	6.7%
Acceptable only if the citizen is suspected of wrong-doing and the surveillance is legally authorised	57.8%	51.9%	13.3%
Acceptable if the citizen is informed	20.0%	17.8%	5.9%
Acceptable if the citizen has given consent	20.0%	23.7%	26.7%
Not acceptable in any circumstances	7.4%	13.3%	42.2%
I don't know	7.0%	0.0%	1.5%

_____

Q7.1: Please indicate the extent to which you believe the following practices of government agencies for fighting crime are acceptable or not: Government agencies share a citizen's information gathered via surveillance measures with […]

Generally, the sharing of information gathered through surveillance by government agencies with other government agencies or with foreign governments is deemed acceptable by the majority of respondents if the citizen is suspected of wrong-doing. However, most of these respondents believe it is necessary that the surveillance needs to be legally authorised for it to be acceptable. About one out of five participants believe it is acceptable for information gathered through surveillance by government agencies to be shared with other government agencies or with foreign governments if the citizen has given consent. Whilst results regarding the sharing of information with other government agencies or foreign governments are fairly similar, sharing information with private companies is much less acceptable even if surveillance has been lawfully authorised for somebody suspected of wrong-doing. Many respondents (42.2%) think it is unacceptable in all circumstances or only if the citizen has given consent (26.7%) for government agencies to share information gathered through surveillance with private companies.

Table 11

Acceptability of data sharing practices of private companies

	Sharing citizens' information gathered via surveillance measures with government agencies	Sharing citizens' information gathered via surveillance measures with foreign governments	Sharing citizens' information gathered via surveillance measures with other private companies
Fully acceptable in all circumstances	5.9%	8.1%	11.1%
Acceptable only if the citizen is suspected of wrong-doing	11.9%	9.6%	4.4%
Acceptable only if the citizen is suspected of wrong-doing and the surveillance is legally authorised	51.1%	27.4%	12.6%
Acceptable if the citizen is informed	18.5%	10.4%	6.7%
Acceptable if the citizen has given consent	20.0%	19.3%	24.4%
Not acceptable in any circumstances	15.6%	34.1%	45.9%
I don't know	0.0%	7.0%	0.0%

_____

Q7.2: Please indicate the extent to which you believe the following practices of private companies for fighting crime are acceptable or not: Private companies share a citizen's information gathered via surveillance measures with […]

There is an even lower number of respondents who find it fully acceptable, or acceptable if the citizen is suspected of wrong-doing, if private companies share a citizen's personal information. Lawfulness still has a strong effect, but it is generally less strong than with government sharing practices. Generally, there is a considerable number of respondents who feel that, unless information or consent has been given, private data should "stay private" – particularly information sharing practices between private companies are deemed unacceptable in any circumstances (45.9%).

7. Acceptability of surveillance in different locations

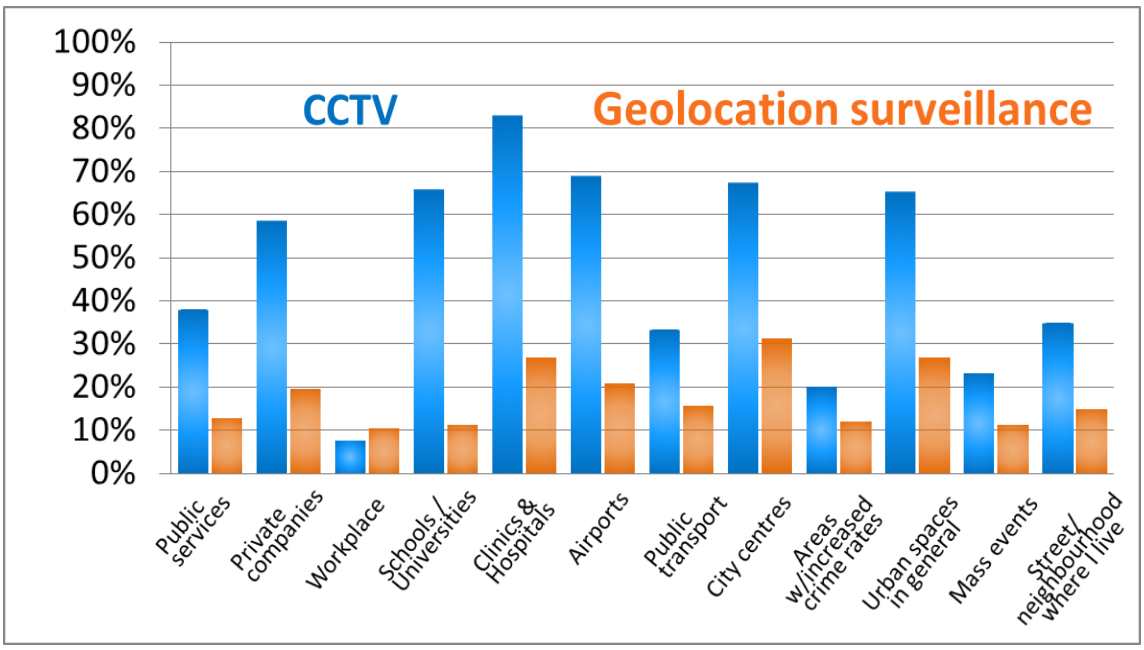

Figure 3: Acceptability of surveillance in different locations
Q6.1 – In which of the following locations or events would you find the different types of surveillance for fighting crime acceptable?

CCTV surveillance is, mostly, perceived as clearly more acceptable than geolocation surveillance for the purposes of fighting crime in all the events and locations investigated, and acceptance rates for CCTV are typically 100 to 200% higher as those for geolocation surveillance.[16] There are mostly no gender differences, with the exceptions of areas with increased crime rates, urban spaces in general, mass events and the own neighbourhood where female respondents find CCTV significantly more acceptable than male respondents.

Both types of surveillance are least accepted in the workplace (CCTV 7%, geolocation surveillance 10%). The highest acceptance of surveillance by CCTV is in clinics and hospitals (83%). A possible explanation for this rather surprising result could be that such acceptance levels of surveillance in clinics and hospitals may be related to high levels of trust in the care provided by these institutions, or to an increased perceived vulnerability in these locations that requires higher levels of protection through surveillance. Acceptance levels for CCTV in airports, city centres, urban spaces in general and schools or universities are also elevated (65-69%), which in itself is unsurprising – but surveillance in specific areas with increased crime rates is much less acceptable (20%). This may be due to respondents having become accustomed to surveillance in city centres and urban areas.

[16] With the exception of workplace surveillance where geolocation surveillance is found to be more acceptable than CCTV, though acceptance for both CCTV and geolocation surveillance in the workplace is extremely low, and surveillance in schools/universities where the acceptance of CCTV is five times higher than the acceptance of geolocation surveillance

8. Economic costs of surveillance

Few respondents believed that the money allocated to government agencies for carrying out surveillance for the purpose of fighting crime in their country is "just right"; 13.3% indicated that, in their opinion, there was too little or far too little money allocated, 25.2% believed it was too much or far too much. But overall more than half of the respondents felt that they, actually, "don't know" whether sufficient funds were allocated to government agencies for carrying out surveillance for the purpose of fighting crime, with female respondents replying far more often "I don't know" than male respondents.

Those respondents who thought that the money allocated to government agencies for carrying out surveillance to fight crime was too little or far too little were asked whether they are prepared to pay higher taxes so that more money can be allocated for this purpose. Less than a quarter of these respondents (22.2%) indicated they would be willing to do so whilst the majority (55.6%) replied that they would not. However, the very low number of respondents to this question (n=18) only allows very limited interpretations of these results.

Table 12
Beliefs about money allocated to surveillance

Q6.2	Total	Female	Male
far too little	5.2%	1.5%	8.8%
too little	8.1%	7.5%	8.8%
just right	8.1%	6.0%	10.3%
too much	14.1%	10.4%	17.6%
far too much	11.1%	6.0%	16.2%
I don't know	52.6%	67.2%	38.2%*
No answer	0.7%	1.5%	0.0%

Q6.2: In your opinion is the money allocated to government agencies for carrying out surveillance for the purpose of fighting crime in your country […]?
Note: Results in this table marked with an asterisk (*) signify that the results between males and females are statistically significantly different (p<.05). Other differences between males and females are not statistically significant.

Table 13
Willingness to pay more taxes to increase budget allocated to carry out surveillance to fight crime

Q6.2.1	Total	Female	Male
Yes	22.2%	16.7%	25%*
No	55.6%	16.7%	75%*
I don't know	16.7%	50.0%	0%*
No answer	5.6%	16.7%	0%*

Q6.2.1: Would you be willing to pay more taxes so that more money is allocated for carrying out surveillance to fight crime?
Note: Results in this table related to gender and marked with an asterisk (*) are statistically significant (p<.05); for all other results the respective tests did not show a statistically significant difference between gender.

9. Social costs of surveillance

9.1 Attitudes towards surveillance

Whilst only a minority of respondents agreed that surveillance may hold social benefits such as the protection of the individual citizen and protection of the community, the risks associated with surveillance seemed to be more keenly felt. The highest perceived risk is privacy invasion through surveillance, followed by the risks that information gathered through surveillance is misinterpreted, intentionally misused, or that surveillance may violate citizens' right to control whether information about them is used. The risks that surveillance may cause discrimination or stigma and limit citizen rights (to communication, free speech and information) also appear to be very strong issues. There were no statistically significant gender differences in the attitudes and perceptions of respondents towards surveillance ("social costs"), except for males agreeing more than females with the statement that surveillance may limit a citizen's right of expression and free speech.

Table 14
Attitudes towards surveillance

		Total		Female		Male	
		Mean	STD	Mean	STD	Mean	STD
Q8.1.1	Surveillance provides protection to the individual citizen	3.33	1.967	3.71	2.051	2.94*	1.810
Q8.1.2	Surveillance provides protection of the community	3.42	1.883	3.69	1.887	3.14	1.853
Q8.1.3	Surveillance can be a source of personal excitement	3.22	2.480	2.71	2.322	3.61	2.548
Q8.1.4	Surveillance can be something to play with	3.03	2.629	3.16	2.655	2.90	2.621
Q8.1.5	Surveillance may cause discrimination towards specific groups of society	6.05	1.666	5.89	1.867	6.20	1.438
Q8.1.6	Surveillance may be a source of stigma	6.11	1.484	5.85	1.725	6.37	1.163
Q8.1.7	Surveillance may violate a person's privacy	6.75	0.835	6.68	0.931	6.82	0.727
Q8.1.8	Surveillance may violate citizens' right to control whether information about them is used	6.52	1.153	6.35	1.381	6.68	0.862
Q8.1.9	There is a potential that information gathered via surveillance could be intentionally misused	6.57	1.084	6.53	1.183	6.61	0.990
Q8.1.10	There is a potential that information gathered via surveillance could be misinterpreted	6.63	0.952	6.53	1.041	6.73	0.851
Q8.1.11	Surveillance may limit a citizen's right of expression and free speech	6.12	1.739	5.80	2.002	6.44*	1.371

Q8.1.12	Surveillance may limit a citizen's right of communication	6.45	1.247	6.29	1.529	6.60	0.880
Q8.1.13	Surveillance may limit a citizen's right of information	6.10	1.684	5.98	1.848	6.21	1.515

Q8.1: Please indicate the extent to which you agree or disagree with the following statements clicking on the point on the scale that best represents your views. (1=disagree; 7=agree)
Note: Results in this table marked with an asterisk (*) signify that the results between males and females are statistically significantly different (p<.05). Other differences between males and females are not statistically significant

9.2 Behavioural changes resulting from surveillance

Despite the Austrian respondents' very high level of risk perception, comparatively few of them have made changes to their behaviour as a result of being aware of surveillance. The two changes in behaviour that were undertaken by a majority of respondents was to stop exchanging their personal data for discounts or vouchers, and keeping themselves informed about technical possibilities to protect their personal data, but only a minority of respondents have taken more proactive moves such as restricting their activities, avoiding surveilled locations or taking defensive measures. In some of these behavioural changes[17], it appears that male respondents are more active, or less inactive, than female respondents.

Table 15
Behaviour changes resulting from an awareness of surveillance

		Total		Female		Male	
		Mean	**STD**	**Mean**	**STD**	**Mean**	**STD**
Q8.2.1	I have restricted my activities or the way I behave	3.90	2.315	3.54	2.240	4.23	2.350
Q8.2.2	I have avoided locations or activities where I suspect surveillance is taking place	3.17	2.144	2.94	2.061	3.41	2.216
Q8.2.3	I have taken defensive measures (hiding face, faking data, incapacitating surveillance device)	2.50	1.984	2.02	1.781	3.00*	2.071
Q8.2.4	I have made fun of it	3.22	2.421	3.10	2.454	3.34	2.402
Q8.2.5	I have filed a complaint with the respective authorities	1.99	1.893	1.92	1.831	2.07	1.965
Q8.2.6	I have informed the media	1.74	1.560	1.54	1.324	1.92	1.744
Q8.2.7	I have promoted or participated in collective actions of counter-surveillance	2.18	1.924	2.11	1.950	2.25	1.910
Q8.2.8	have kept myself informed about technical possibilities to protect my personal data	4.95	1.937	4.36	1.989	5.55*	1.696

[17] Taking defensive measures and keeping oneself informed about technical possibilities to protect one's personal data.

Q8.2.9	I have stopped accepting discounts or vouchers if they are in exchange for my personal data	5.19	2.186	5.11	2.240	5.27	2.145

Q8.2: To what extent has your awareness of surveillance changed your personal behaviour? Please indicate the extent to which you agree or disagree with the following statements clicking on the point on the scale that best represents your views. (1=disagree; 7=agree)
Note: Results in this table marked with an asterisk (*) signify that the results between males and females are statistically significantly different (p<.05). Other differences between males and females are not statistically significant.

9.3 Perceived social benefits and social costs: Relationships

The two perceived social benefits, protection for the individual citizen and protection for the community, are strongly related to each other. Many respondents have the same beliefs about both these benefits. However, these perceived benefits appear to be largely independent of the perceived social costs, with the exception of a moderate negative relationship between surveillance providing protection of the individual citizen and surveillance potentially being a cause of discrimination.

Several respondents have the same attitude towards many of the perceived social costs, being likely to respond in the same manner as to

- whether surveillance limits the rights of free speech, communication and information;
- the potential for surveillance to violate privacy and violate the right of citizens to control whether information collected about them through surveillance is used;
- the potential of privacy violation and the potential of data misinterpretation;
- surveillance violating the right of citizens to control whether information collected about them through surveillance is used and surveillance potentially being a cause of discrimination;
- potential misinterpretation and surveillance being a potential source of stigma;
- and surveillance bearing the risk of discrimination and being a source of stigma (see table A3 in Appendix A).

Additionally, there is a moderate to strong relationship between the perceived social benefits of individual and community protection and the perceived usefulness and effectiveness of most types of surveillance measures investigated in this study (see table A6 in Appendix A). The strongest link, here, can be seen between surveillance providing protection for the community and the usefulness of social-networking surveillance for detection of crime.

There are some moderate to strong links between changes in different behaviours as a result of awareness of surveillance. The strongest connections are between participating in collective actions of counter-surveillance and informing the media, and between avoiding locations where surveillance is suspected to take place and restricting one's activities (see Table A4 in Appendix A). These can be seen to represent certain "strategies" of protection against surveillance, the latter being largely described as the "chilling effect" of surveillance, though it needs to be kept in mind that few respondents have acted in this way (see Table 15 above). Those changes of personal behaviour most often indicated by respondents - not accepting discounts/vouchers in exchange for personal data, and keeping oneself informed about the possibilities of technical data protection – are only weakly related to the other forms of behavioural changes[18] (see Table A4 in Appendix A).

[18] With the exception of a moderate relationship between stopping to accept vouchers, restricting activities and avoiding locations.

In this study there is little evidence to support a relationship between the perceived negative effects of surveillance and behavioural changes as a result of surveillance (see table A5 in Appendix A). Those social costs which were perceived most often – data misuse, data misinterpretation, violation of privacy and violation of the right to control the use of one's personal data – show only weak relationships with not accepting vouchers in exchange for personal data, and no relationship with other behavioural measures that could, perhaps, be expected in such case (e.g., filing complaints with the responsible authorities).

10. Conclusion

Overall, the Austrian respondents felt more insecure than secure in the presence of surveillance, and they indicated a strongly felt lack of trust in the protection of, and control over, personal information gathered via surveillance.

Based on the data collected in this study, the majority of Austrian respondents also feel more unhappy than happy with the different types of surveillance investigated, and they feel also unhappy about surveillance taking place without them knowing about it. Additionally, there is a link between feeling happy, or unhappy, about surveillance and feeling secure or insecure through the presence of surveillance.

However, analyses also indicate that increasing the perceived effectiveness of surveillance measures and, in particular, increasing the perceived effectiveness of laws regarding the protection of personal data gathered via surveillance may make citizens feel more secure.

Further research is needed to disentangle the relationships and effects between surveillance measures, feelings of security or insecurity, and citizens' general quality of life feelings.

APPENDICES

Appendix A – Figures and tables

Table A1: Correlations – Usefulness for reduction, detection and prosecution of crime

Usefulness for **REDUCTION** of crime

			CCTV	Database	SNS	financialT	geolocat.
			Q3.1_1	Q3.1_2	Q3.1_3	Q3.1_4	Q3.1_5
REDUCTION	CCTV	Q3.1_1	1.000	0.419	0.347	0.185	0.465
	database	Q3.1_2	0.419	1.000	0.678	0.430	0.602
	SNS	Q3.1_3	0.347	0.678	1.000	0.301	0.542
	financT	Q3.1_4	0.185	0.430	0.301	1.000	0.375
	Geoloc.	Q3.1_5	0.465	0.602	0.542	0.375	1.000
DETECTION	CCTV	Q3.2_1	0.637	0.423	0.338	0.257	0.489
	database	Q3.2_2	0.493	0.743	0.548	0.336	0.589
	SNS	Q3.2_3	0.453	0.612	0.801	0.237	0.546
	financT	Q3.2_4	0.302	0.435	0.268	0.643	0.371
	Geoloc.	Q3.2_5	0.497	0.610	0.485	0.308	0.556
PROSECUTION	CCTV	Q3.3_1	0.524	0.434	0.400	0.117	0.411
	database	Q3.3_2	0.535	0.688	0.530	0.267	0.474
	SNS	Q3.3_3	0.450	0.532	0.614	0.242	0.406
	financT	Q3.3_4	0.283	0.381	0.260	0.537	0.304
	Geoloc.	Q3.3_5	0.488	0.503	0.431	0.232	0.527

Usefulness for **DETECTION** of crime

			CCTV	Database	SNS	financialT	geolocat.
			Q3.2_1	Q3.2_2	Q3.2_3	Q3.2_4	Q3.2_5
DETECTION	CCTV	Q3.2_1	1.000	0.542	0.507	0.479	0.646
	database	Q3.2_2	0.542	1.000	0.655	0.496	0.677
	SNS	Q3.2_3	0.507	0.655	1.000	0.372	0.547
	financT	Q3.2_4	0.479	0.496	0.372	1.000	0.496
	Geoloc.	Q3.2_5	0.646	0.677	0.547	0.496	1.000
PROSECUTION	CCTV	Q3.3_1	0.596	0.451	0.472	0.285	0.514
	database	Q3.3_2	0.439	0.691	0.562	0.428	0.539
	SNS	Q3.3_3	0.415	0.468	0.642	0.289	0.430
	financT	Q3.3_4	0.354	0.313	0.286	0.627	0.276
	Geoloc.	Q3.3_5	0.550	0.511	0.397	0.432	0.550

Usefulness for **PROSECUTION** of crime

			CCTV	Database	SNS	financialT	geolocat.
			Q3.3_1	Q3.3_2	Q3.3_3	Q3.3_4	Q3.3_5
PROSECUTION	CCTV	Q3.3_1	1.000	0.588	0.512	0.312	0.578
	database	Q3.3_2	0.588	1.000	0.652	0.461	0.655
	SNS	Q3.3_3	0.512	0.652	1.000	0.468	0.535
	financT	Q3.3_4	0.312	0.461	0.468	1.000	0.478
	Geoloc.	Q3.3_5	0.578	0.655	0.535	0.478	1.000

Table A2: Correlations – Usefulness and happiness / feeling of security

			HAPPINESS with surveillance					Feeling of SECURITY
			CCTV	Database	SNS	FinancT	Geoloc.	
			Q5.3_1	Q5.3_3	Q5.3_2	Q5.3_4	Q5.3_5	Q4.3
Usefulness for **REDUCTION** of crime	**CCTV**	Q3.1_1	-0.576	-0.294	-0.258	-0.234	-0.430	0.435
	database	Q3.1_2	-0.352	-0.471	-0.408	-0.296	-0.482	0.511
	SNS	Q3.1_3	-0.349	-0.526	-0.363	-0.279	-0.417	0.44
	financialT	Q3.1_4	-0.030	-0.244	-0.205	-0.398	-0.227	0.318
	geolocat.	Q3.1_5	-0.379	-0.459	-0.320	-0.345	-0.500	0.543
Usefulness for **DETECTION** of crime	**CCTV**	Q3.2_1	-0.538	-0.392	-0.282	-0.318	-0.448	0.483
	database	Q3.2_2	-0.452	-0.413	-0.312	-0.316	-0.471	0.542
	SNS	Q3.2_3	-0.446	-0.514	-0.354	-0.279	-0.470	0.558
	financialT	Q3.2_4	-0.265	-0.326	-0.308	-0.458	-0.397	0.425
	geolocat.	Q3.2_5	-0.456	-0.433	-0.331	-0.320	-0.530	0.484
Usefulness for **PROSECUTION** of crime	**CCTV**	Q3.3_1	-0.513	-0.326	-0.278	-0.296	-0.430	0.391
	database	Q3.3_2	-0.402	-0.338	-0.349	-0.210	-0.389	0.418
	SNS	Q3.3_3	-0.354	-0.432	-0.271	-0.228	-0.345	0.368
	financialT	Q3.3_4	-0.176	-0.243	-0.279	-0.479	-0.244	0.311
	geolocat.	Q3.3_5	-0.457	-0.330	-0.307	-0.269	-0.419	0.333

Table A3: Correlations – Social costs (perceptions)

Social costs I (perceptions)		Protection of individual citizen	Protection of community	Source of excitement	Something to play with	Cause of discrimination	Source of stigma	Violates privacy	Violates right to control data	Potential misuse	Potential mis-interpretation	Limits right of free speech	Limits right of communi cation	Limits right of information
		Q8.1_1	Q8.1_2	Q8.1_3	Q8.1_4	Q8.1_5	Q8.1_6	Q8.1_7	Q8.1_8	Q8.1_9	Q8.1_10	Q8.1_11	Q8.1_12	Q8.1_13
Protection individual citizen	Q8.1_1	1.000												
Protection of community	Q8.1_2	0.792	1.000											
Source of excitement	Q8.1_3	0.217	0.281	1.000										
Something to play with	Q8.1_4	0.137	0.186	0.487	1.000									
Cause of discrimi-nation	Q8.1_5	-0.458	-0.351	0.067	0.020	1.000								
Source of stigma	Q8.1_6	-0.324	-0.284	0.064	-0.012	0.646	1.000							
Violates privacy	Q8.1_7	-0.344	-0.258	-0.020	0.024	0.503	0.580	1.000						
Violates right of control data	Q8.1_8	-0.414	-0.220	0.144	0.048	0.649	0.528	0.694	1.000					
Potential misuse	Q8.1_9	-0.160	-0.118	0.090	0.012	0.511	0.606	0.469	0.340	1.000				
Potential mis-interpre-tation	Q8.1_10	-0.274	-0.256	0.059	0.083	0.509	0.644	0.691	0.550	0.492	1.000			
Limits right of free speech	Q8.1_11	-0.345	-0.278	0.142	-0.039	0.631	0.537	0.538	0.605	0.464	0.359	1.000		
Limits right of communi-cation	Q8.1_12	-0.318	-0.268	0.130	0.075	0.572	0.608	0.648	0.580	0.548	0.474	0.732	1.000	
Limits right of information	Q8.1_13	-0.318	-0.275	0.047	-0.024	0.575	0.479	0.424	0.560	0.440	0.294	0.696	0.500	1.000

Table A4: Correlations – Social costs (behaviour)

Social costs II (behaviour)		restricted activities	avoided locations	defensive measures	made fun of it	filed complaint	informed the media	counter-surveillance	info about technical protection	stopped accepting vouchers
		Q8.2_1	Q8.2_2	Q8.2_3	Q8.2_4	Q8.2_5	Q8.2_6	Q8.2_7	Q8.2_8	Q8.2_9
restricted activities	Q8.2_1	1.000								
avoided locations	Q8.2_2	0.602	1.000							
defensive measures	Q8.2_3	0.413	0.516	1.000						
made fun of it	Q8.2_4	0.001	0.176	0.255	1.000					
filed complaint	Q8.2_5	0.184	0.374	-0.004	0.169	1.000				
informed the media	Q8.2_6	0.181	0.309	0.164	0.207	0.565	1.000			
counter-surveillance	Q8.2_7	0.088	0.331	0.236	0.303	0.422	0.612	1.000		
info about technical protection	Q8.2_8	0.313	0.301	0.313	0.059	0.145	0.292	0.304	1.000	
stopped accepting vouchers	Q8.2_9	0.429	0.439	0.285	0.134	0.270	0.187	0.128	0.105	1.000

Table A5: Correlations – Social costs (perceptions vs. behaviour)

Social costs III (perceptions vs behaviour)		restricted activities	avoided locations	defensive measures	made fun of it	filed complaint	informed the media	counter-surveillance	info about technical protection	stopped accepting vouchers
		Q8.2_1	Q8.2_2	Q8.2_3	Q8.2_4	Q8.2_5	Q8.2_6	Q8.2_7	Q8.2_8	Q8.2_9
Protection of individual citizen	Q8.1_1	-0.244	-0.284	-0.222	-0.122	-0.173	-0.173	-0.208	-0.230	-0.206
Protection of community	Q8.1_2	-0.251	-0.308	-0.246	-0.124	-0.221	-0.220	-0.197	-0.245	-0.334
Source of excitement	Q8.1_3	0.023	-0.112	0.129	0.058	-0.093	0.060	-0.018	0.007	-0.252
Something to play with	Q8.1_4	0.048	-0.029	0.065	-0.095	-0.081	-0.155	-0.168	-0.015	-0.097
Cause of discrimination	Q8.1_5	0.294	0.244	0.186	0.293	0.154	0.129	0.157	0.326	0.117
Source of stigma	Q8.1_6	0.130	0.245	0.233	0.303	0.101	0.073	0.061	0.248	0.124
Violates privacy	Q8.1_7	0.203	0.123	0.107	0.096	-0.036	-0.089	0.040	0.282	0.065
Violates right to control data	Q8.1_8	0.316	0.153	0.149	0.164	0.098	0.068	0.022	0.333	0.005
Potential misuse	Q8.1_9	0.172	0.079	0.152	0.148	0.035	-0.010	0.047	0.373	0.152
Potential misinterpretation	Q8.1_10	0.252	0.153	0.133	0.175	-0.009	-0.043	-0.010	0.326	0.094
Limits right of free speech	Q8.1_11	0.294	0.291	0.240	0.178	0.157	0.143	0.209	0.403	0.128
Limits right of communi cation	Q8.1_12	0.198	0.228	0.182	0.244	0.128	0.096	0.096	0.316	0.081
Limits right of information	Q8.1_13	0.310	0.276	0.205	0.034	0.056	0.161	0.110	0.340	0.145

Table A6: Correlations – Social benefits, usefulness and effectiveness of surveillance

			individual citizen	community
			Q8.1_1	Q8.1_2
Usefulness for **REDUCTION** of crime	**CCTV**	Q3.1_1	0.491	0.586
	database	Q3.1_2	0.496	0.55
	SNS	Q3.1_3	0.383	0.552
	financialT	Q3.1_4	0.227	0.212
	geolocat.	Q3.1_5	0.517	0.586
Usefulness for **DETECTION** of crime	**CCTV**	Q3.2_1	0.42	0.529
	database	Q3.2_2	0.535	0.583
	SNS	Q3.2_3	0.461	0.659
	financialT	Q3.2_4	0.337	0.271
	geolocat.	Q3.2_5	0.445	0.52
Usefulness for **PROSECUTION** of crime	**CCTV**	Q3.3_1	0.436	0.449
	database	Q3.3_2	0.475	0.466
	SNS	Q3.3_3	0.294	0.438
	financialT	Q3.3_4	0.198	0.186
	geolocat.	Q3.3_5	0.431	0.434
EFFECTIVENESS	**CCTV**	Q5.1.1_1	0.518	0.592
	database	Q5.1.1_2	0.513	0.537
	SNS	Q5.1.1_3	0.455	0.592
	financialT	Q5.1.1_4	0.362	0.341
	geolocat.	Q5.1.1_5	0.559	0.553

Table A7: Correlations – Social costs and privacy in surveillance

		Surveillance measures having a negative impact on privacy				
		Q5.1.2_1	Q5.1.2_2	Q5.1.2_3	Q5.1.2_4	Q5.1.2_5
	Social costs (perceptions)	**CTV**	**Databases**	**SNS**	**FinTrac**	**Geoloc.**
Q8.1_1	Protection individual citizen	-0.390	-0.338	-0.334	-0.273	-0.436
Q8.1_2	Protection of community	-0.461	-0.413	-0.363	-0.282	-0.479
Q8.1_3	Source of excitement	-0.126	-0.088	-0.027	0.130	-0.069
Q8.1_4	Something to play with	-0.108	-0.078	-0.081	0.071	-0.112
Q8.1_5	Cause of discrimination	0.307	0.267	0.428	0.399	0.486
Q8.1_6	Source of stigma	0.309	0.307	0.311	0.306	0.463
Q8.1_7	Violates privacy	0.250	0.234	0.250	0.098	0.342
Q8.1_8	Violates right of control data	0.279	0.261	0.410	0.242	0.363
Q8.1_9	Potential misuse	0.188	0.200	0.184	0.266	0.304
Q8.1_10	Potential misinterpretation	0.318	0.326	0.312	0.222	0.391
Q8.1_11	Limits right of free speech	0.368	0.325	0.379	0.328	0.311
Q8.1_12	Limits right of communication	0.253	0.270	0.276	0.225	0.301
Q8.1_13	Limits right of information	0.342	0.364	0.376	0.412	0.328
	Social costs (behaviour)					
Q8.2_1	restricted activities	0.312	0.255	0.338	0.162	0.295
Q8.2_2	avoided locations	0.304	0.304	0.182	0.288	0.240
Q8.2_3	defensive measures	0.372	0.236	0.218	0.254	0.231
Q8.2_4	made fun of it	0.158	0.214	0.167	0.118	0.232
Q8.2_5	filed complaint	0.202	0.165	0.232	0.202	0.214
Q8.2_6	informed the media	0.179	0.111	0.144	0.232	0.121
Q8.2_7	counter-surveillance	0.196	0.192	0.142	0.235	0.186
Q8.2_8	info about technical protection	0.377	0.309	0.321	0.288	0.247
Q8.2_9	stopped accepting vouchers	0.224	0.264	0.142	0.111	0.180

Table A8: Correlations – Usefulness vs. effectiveness of surveillance

			EFFECTIVENESS against crime				
			CCTV	**Database**	**SNS**	**FinancT**	**Geoloc.**
			Q5.1.1_1	Q5.1.1_2	Q5.1.1_3	Q5.1.1_4	Q5.1.1_5
Usefulness for	**REDUCTION**	**CCTV**	Q3.1_1	0.735	0.435	0.418	0.309	0.515
		database	Q3.1_2	0.556	0.753	0.605	0.442	0.654
		SNS	Q3.1_3	0.388	0.480	0.730	0.196	0.529
		financT	Q3.1_4	0.215	0.340	0.318	0.691	0.354
		Geoloc.	Q3.1_5	0.510	0.527	0.609	0.347	0.638
	DETECTION	**CCTV**	Q3.2_1	0.729	0.476	0.466	0.368	0.527
		database	Q3.2_2	0.627	0.755	0.577	0.445	0.621
		SNS	Q3.2_3	0.492	0.568	0.812	0.300	0.562
		financT	Q3.2_4	0.392	0.473	0.391	0.706	0.417
		Geoloc.	Q3.2_5	0.700	0.552	0.537	0.382	0.612
	PROSECUTION	**CCTV**	Q3.3_1	0.644	0.449	0.412	0.329	0.439
		database	Q3.3_2	0.537	0.615	0.491	0.381	0.530
		SNS	Q3.3_3	0.432	0.497	0.615	0.286	0.450
		financT	Q3.3_4	0.290	0.341	0.294	0.590	0.279
		Geoloc.	Q3.3_5	0.595	0.502	0.411	0.380	0.612

Table A9: Correlations – Security and happiness

				Feeling of **HAPPINESS**					
			Feeling of **SECURITY**	**CCTV**	**SNS**	**Database**	**FinancT**	**Geoloc.**	Happiness about **NOT KNOWING**
			Q4.3	Q5.3_1	Q5.3_2	Q5.3_3	Q5.3_4	Q5.3_5	Q5.4
Feeling of **SECURITY**		Q4.3	1.000						
Feeling of **HAPPINESS**	**CCTV**	Q5.3_1	-0.499	1.000					
	SNS	Q5.3_2	-0.534	0.523	1.000				
	Database	Q5.3_3	-0.444	0.484	0.663	1.000			
	FinancT	Q5.3_4	-0.381	0.453	0.536	0.495	1.000		
	Geoloc.	Q5.3_5	-0.599	0.630	0.672	0.640	0.480	1.000	
Happiness about **NOT KNOWING**		Q5.4	-0.380	0.442	0.509	0.495	0.435	0.498	1.000

Table A10: Correlations – Impact on privacy and feelings of security, trust and control

		NEGATIVE IMPACT on PRIVACY				
		CCTV	database	SNS	financialT	geolocat.
		Q5.1.2_1	Q5.1.2_2	Q5.1.2_3	Q5.1.2_4	Q5.1.2_5
Feeling of security	Q4.3	-0.514	-0.531	-0.437	-0.374	-0.482
Feeling of control I	Q4.4.1	-0.148	-0.198	-0.162	-0.119	-0.186
Feeling of control II	Q4.4.2	-0.076	-0.186	-0.137	-0.132	-0.088
Trust I	Q4.5.1	-0.446	-0.495	-0.427	-0.373	-0.404
Trust II	Q4.5.2	-0.259	-0.396	-0.263	-0.248	-0.354

Table A11: Correlations – Feelings of security, trust and control vs. effectiveness of laws

		Knowledge of laws	Effective-ness of laws	Feeling of security	Feeling of control I	Feeling of control II	Trust I	Trust II
		Q4.1	Q4.2	Q4.3	Q4.4.1	Q4.4.2	Q4.5.1	Q4.5.2
Knowledge of laws	Q4.1	1.000						
Effectiveness of laws	Q4.2	0.147	1.000					
Feeling of security	Q4.3	0.078	0.573	1.000				
Feeling of control I	Q4.4.1	0.058	0.294	0.301	1.000			
Feeling of control II	Q4.4.2	0.077	0.171	0.344	0.461	1.000		
Trust I	Q4.5.1	0.026	0.424	0.500	0.445	0.338	1.000	
Trust II	Q4.5.2	-0.092	0.175	0.324	0.261	0.466	0.364	1.000

Table A12: Correlations – Feelings of security, trust and control vs. effectiveness of surveillance measures

		EFFECTIVENESS				
		CCTV	database	SNS	financialT	geolocat.
		Q5.1.1_1	Q5.1.1_2	Q5.1.1_3	Q5.1.1_4	Q5.1.1_5
Feeling of security	Q4.3	0.505	0.499	0.552	0.427	0.486
Feeling of control I	Q4.4.1	0.294	0.297	0.364	0.282	0.28
Feeling of control II	Q4.4.2	0.225	0.269	0.34	0.281	0.214
Trust I	Q4.5.1	0.395	0.378	0.418	0.42	0.408
Trust II	Q4.5.2	0.13	0.353	0.204	0.178	0.106

Appendix B – Questionnaire

Q0.1 Country of Residence

1. Austria
2. Belgium
3. Bulgaria
4. Croatia
5. Cyprus
6. Czech Republic
7. Denmark
8. Estonia
9. Finland
10. France
11. Germany
12. Greece
13. Hungary
14. Ireland
15. Italy
16. Latvia
17. Lithuania
18. Luxembourg
19. Malta
20. Netherlands
21. Norway
22. Poland
23. Portugal
24. Romania
25. Slovakia
26. Slovenia
27. Spain
28. Sweden
29. United Kingdom
30. Other _____ *(please write in)*

Q0.2 Age

[ ] years

Q0.3 Gender

1. Female

2. Male
3. Other

Q1 Have you heard of the use of any of the below for the purpose of monitoring, observing or tracking of people's behaviour, activities or personal information?

1. Biometric data, e.g. analysis of fingerprints, palm prints, facial or body features
2. "Suspicious" behaviour, e.g. automated detection and analysis of raised voices, facial expressions, aggressive gestures
3. Data and traffic on the internet, e.g. Deep Packet/Content Inspection
4. Databases containing personal information, e.g. searching state pension databases, or customer databases of private companies
5. Online communication, e.g. social network analysis, monitoring of chat rooms or forums
6. Telecommunication, e.g. monitoring of phone calls or SMS
7. Electronic tagging / Radio Frequency Identification (RFID), e.g. tracking geolocation with electronic chips implanted under the skin or in bracelets
8. Global Positioning Systems (GPS), e.g. tracking geolocation of cars or mobile phones
9. CCTV cameras, e.g. in public places, airports or supermarkets
10. Financial information, e.g. tracking of debit/credit card transactions

From now on, in all questions, the word "surveillance" is used for the monitoring, observing or tracking of people's behaviour, activities or personal information.

Q2 What reasons for the setting up of surveillance do you know of?

1. The reduction of crime
2. The detection of crime
3. The prosecution of crime
4. Control of border-crossings
5. Control of crowds
6. Other *(please write in)* _____
7. I Don't know of any reasons.

Q3.1 How useful in general do you think the following types of surveillance are for the <u>reduction</u> of crime?

CCTV cameras	1 Not at all useful	2	3	4	5 Very useful	I don't know
Surveillance using databases containing personal information	1 Not at all useful	2	3	4	5 Very useful	I don't know
Surveillance of online social networking	1 Not at all useful	2	3	4	5 Very useful	I don't know
Surveillance of financial transactions	1 Not at all useful	2	3	4	5 Very useful	I don't know
Geolocation surveillance (Using mobile phones, GPS, electronic tagging, or RFID to determine the location of the devices and the devices' owners)	1 Not at all useful	2	3	4	5 Very useful	I don't know

Q3.2 How useful in general do you think the following types of surveillances are for the <u>detection</u> of crime?

CCTV cameras	1 Not at all useful	2	3	4	5 Very useful	I don't know
Surveillance using databases containing personal information	1 Not at all useful	2	3	4	5 Very useful	I don't know
Surveillance of online social networking	1 Not at all useful	2	3	4	5 Very useful	I don't know
Surveillance of financial transactions	1 Not at all useful	2	3	4	5 Very useful	I don't know
Geolocation surveillance (Using mobile phones, GPS, electronic tagging, or RFID to determine the location of the devices and the devices' owners)	1 Not at all useful	2	3	4	5 Very useful	I don't know

Q3.3 How useful in general do you think the following types of surveillance are for the <u>prosecution</u> of crime?

CCTV cameras	1 Not at all useful	2	3	4	5 Very useful	I don't know
Surveillance using databases containing personal information	1 Not at all useful	2	3	4	5 Very useful	I don't know
Surveillance of online social networking	1 Not at all useful	2	3	4	5 Very useful	I don't know
Surveillance of financial transactions	1 Not at all useful	2	3	4	5 Very useful	I don't know
Geolocation surveillance (Using mobile phones, GPS, electronic tagging, or RFID to determine the location of the devices and the devices' owners)	1 Not at all useful	2	3	4	5 Very useful	I don't know

Q4.1 How much do you know about the laws and regulations of your country regarding the protection of your personal information gathered via surveillance measures?
1=I don't know anything about such laws and regulations, 5=I am very well informed

Q4.2 How effective do you find these laws and regulations?
1=not effective at all, 5=very effective, I don't know

Q4.3 How secure does the presence of surveillance measures make you feel?
1=very insecure, 5=very secure, I don't know

Q4.4.1 How much control do you think you have over the processing of your personal information gathered via <u>government agencies</u>?
1=no control, 5=full control, I don't know

Q4.4.2 How much control do you think you have over the processing of your personal information gathered via <u>private companies</u>?
1=no control, 5=full control, I don't know

Q4.5.1 How much do you trust <u>government agencies</u> that they protect your personal information gathered via surveillance measures?
1=no trust, 5=complete trust, I don't know

Q4.5.2 How much do you trust <u>private companies</u> that they protect your personal information gathered via surveillance measures?
1=no trust, 5=complete trust, I don't know

Q5.1.1 Please indicate the extent to which you agree or disagree with the following statements clicking on the point on the scale that best represents your views.
(1=disagree, 7=agree, I don't know)

Q5.1.1.1 CCTV is an effective way to protect against crime.
Q5.1.1.2 Surveillance utilising databases containing personal information is an effective way to protect against crime.
Q5.1.1.3 Surveillance of online social-networking is an effective way to protect against crime.
Q5.1.1.4 Surveillance of financial transactions is an effective way to protect against crime.
Q5.1.1.5 Geolocation surveillance using mobile phones, GPS, electronic tagging, or RFID is an effective way to protect against crime.

Q5.1.2 Please indicate the extent to which you agree or disagree with the following statements clicking on the point on the scale that best represents your views.
(1=disagree, 7=agree, I don't know)

Q5.1.2.1 CCTV aimed at protection against crime has a negative impact on my privacy.
Q5.1.2.2 Surveillance utilising databases containing personal information aimed at protection against crime has a negative impact on my privacy.
Q5.1.2.3 Surveillance of online social-networking aimed at protection against crime has a negative impact on my privacy.
Q5.1.2.4 Surveillance of financial transactions aimed at protection against crime has a negative impact on my privacy.
Q5.1.2.5 Geolocation surveillance using mobile phones, GPS, electronic tagging, or RFID aimed at protection against crime has a negative impact on my privacy.

Q5.1.3 Would you be willing to accept payment as compensation for greater invasion of your privacy, using:

	Yes	No	I don't know
Surveillance via CCTV cameras			
Surveillance of online social networks			
Surveillance utilising databases containing personal information			
Surveillance of financial transactions			
Geolocation surveillance (Using mobile phones, GPS, electronic tagging, or RFID to determine the location of the devices and the devices' owners)			

Q5.2.1 Which of the following best describes you?

1. I never notice CCTV cameras.
2. I rarely notice CCTV cameras.
3. I sometimes notice CCTV cameras.
4. I often notice CCTV cameras.
5. I always notice CCTV cameras.
6. I don't know.

Q5.2.2 In your opinion, how often do the following types of surveillance take place in the country where you live?

	Never happens	Rarely happens	Sometimes happens	Often happens	Happens all the time	I don't know
Surveillance via CCTV cameras						
Surveillance of online social networks						
Surveillance utilising databases containing personal information						
Surveillance of financial transactions						
Geolocation surveillance (Using mobile phones, GPS, electronic tagging, or RFID)						

Q5.3 How happy or unhappy do you feel about the following types of surveillance?

	Very happy	Happy	Neither happy nor unhappy	Unhappy	Very unhappy	I don't know
CCTV cameras						
Surveillance of online social networks						
Surveillance utilising databases containing personal information						
Surveillance of financial transactions						
Geolocation surveillance (Using mobile phones, GPS, electronic tagging, or RFID)						

Q5.4 Surveillance may take place without people knowing about it. How do you feel about this?

1. I feel very happy about this.
2. I feel happy about this.
3. I feel neither happy nor unhappy about this.
4. I feel unhappy about this.
5. I feel very unhappy about this.
6. I don't know.

Q6.1 In which of the following locations or events would you find the different types of surveillance for fighting crime acceptable?

	CCTV	**Geolocation surveillance** (Using mobile phones, GPS, electronic tagging, or RFID to determine the location of the devices and the devices' owners)
Public services (e.g. local council offices)	□ Acceptable □ Unacceptable □ I don't know	□ Acceptable □ Unacceptable □ I don't know
Private companies (e.g. banks)	□ Acceptable □ Unacceptable □ I don't know	□ Acceptable □ Unacceptable □ I don't know
Workplace	□ Acceptable □ Unacceptable □ I don't know	□ Acceptable □ Unacceptable □ I don't know
Schools / universities	□ Acceptable □ Unacceptable □ I don't know	□ Acceptable □ Unacceptable □ I don't know
Clinics and hospitals	□ Acceptable □ Unacceptable □ I don't know	□ Acceptable □ Unacceptable □ I don't know
Airports	□ Acceptable □ Unacceptable □ I don't know	□ Acceptable □ Unacceptable □ I don't know
Public transport (Railway, subway, buses, taxis etc.)	□ Acceptable □ Unacceptable □ I don't know	□ Acceptable □ Unacceptable □ I don't know
City centres	□ Acceptable □ Unacceptable □ I don't know	□ Acceptable □ Unacceptable □ I don't know
Specific areas that experience increased crime rates	□ Acceptable □ Unacceptable □ I don't know	□ Acceptable □ Unacceptable □ I don't know
Urban spaces in general	□ Acceptable □ Unacceptable □ I don't know	□ Acceptable □ Unacceptable □ I don't know
Mass events (concerts, football games etc.)	□ Acceptable □ Unacceptable □ I don't know	□ Acceptable □ Unacceptable □ I don't know
The street/neighbourhood where I live	□ Acceptable □ Unacceptable □ I don't know	□ Acceptable □ Unacceptable □ I don't know

Q6.2 In your opinion is the money allocated to government agencies for carrying out surveillance for the purpose of fighting crime in your country

(1=far too little, 2= too little, 3=just right, 4=too much, 5=far too much, 9=I don't know)

Q7.1 Please indicate the extent to which you believe the following practices of <u>government agencies</u> for fighting crime are acceptable or not acceptable.

You may choose more than one option if applicable.

	Fully acceptable in all circumstances	Acceptable only if the citizen is suspected of wrongdoing	Acceptable if the citizen is suspected of wrongdoing and the surveillance is legally authorised	Acceptable if the citizen is informed	Acceptable if the citizen has given consent	Not acceptable in any circumstances	I don't know
Government agencies share a citizen's personal information gathered via surveillance measures **with other government agencies**							
Government agencies share a citizen's personal information gathered via surveillance measures **with foreign governments**							
Government agencies share a citizen's personal information gathered via surveillance measures **with private companies**							

Q7.2 Please indicate the extent to which you believe the following practices of <u>private companies</u> for fighting crime are acceptable or not acceptable.

You may choose more than one option if applicable.

	Fully acceptable in all circumstances	Acceptable only if the citizen is suspected of wrongdoing	Acceptable if the citizen is suspected of wrongdoing and the surveillance is legally authorised	Acceptable if the citizen is informed	Acceptable if the citizen has given consent	Not acceptable in any circumstances	I don't know
Private companies share a citizen's personal information gathered via surveillance measures **with government agencies**							
Private companies share a citizen's personal information gathered via surveillance measures **with foreign governments**							
Private companies share a citizen's personal information gathered via surveillance measures **with other private companies**							

Q8.1 Please indicate the extent to which you agree or disagree with the following statements clicking on the point on the scale that best represents your views.
(1=disagree, 7=agree, I don't know)

Q8.1.1 Surveillance provides protection for the individual citizen.
Q8.1.2 Surveillance provides protection of the community.
Q8.1.3 Surveillance can be a source of personal excitement.
Q8.1.4 Surveillance can be something to play with.
Q8.1.5 Surveillance may cause discrimination towards specific groups of society.
Q8.1.6 Surveillance may be a source of stigma.
Q8.1.7 Surveillance may violate a person's privacy.
Q8.1.8 Surveillance may violate citizens' right to control whether information about them is used.
Q8.1.9 There is a potential that information gathered via surveillance could be intentionally misused by those who collect or process the data.
Q8.1.10 There is a potential that information gathered via surveillance could be misinterpreted by those who collect or process the data.
Q8.1.11 Surveillance may limit a citizen's right of expression and free speech.
Q8.1.12 Surveillance may limit a citizen's right of communication.
Q8.1.13 Surveillance may limit a citizen's right of information.

Q8.2 To what extent has your awareness of surveillance changed your personal behaviour? Please indicate the extent to which you agree or disagree with the following statements clicking on the point on the scale that best represents your views.
(1=disagree, 7=agree, I don't know)

Q8.2.1 I have restricted my activities or the way I behave.
Q8.2.2 I have avoided locations or activities where I suspect surveillance is taking place.
Q8.2.3 I have taken defensive measures such has hiding my face, faking my data, or incapacitating the surveillance device.
Q8.2.4 I have made fun of it.
Q8.2.5 I have filed a complaint with the respective authorities.
Q8.2.6 I have informed the media.
Q8.2.7 I have promoted or participated in collective actions of counter-surveillance, such as using mobile phones to document the behaviour of police and security forces.
Q8.2.8 I have kept myself informed about technical possibilities to protect my personal data.
Q8.2.9 I have stopped accepting discounts or vouchers if they are in exchange for my personal data.

Q9 Demographics

This section relates to information about you. It may be left blank but it would greatly assist our research if you do complete it. If you do not wish to answer these questions please click on the "SUBMIT" button at the bottom of the screen. Thank you.

Q9.1 What is your highest level of education?

1. No formal schooling
2. Primary school
3. Secondary school/High School
4. Tertiary education (University, Technical College, etc.)
5. Post-graduate

Q9.2 Would you say you live in an area with increased security risks?

1. Yes
2. No
3. Not sure/don't know

Q9.3 How often do you usually travel abroad per year?

1. Up to once a year
2. 2-5 times a year
3. 6-10 times a year
4. More than 10 times a year

Q9.4 How often do you usually visit a mass event (concert, sports event, exhibition/fair etc.) per year?

1. Up to once a year
2. 2-5 times a year
3. 6-10 times a year
4. More than 10 times a year

Q9.5 If you make use of the internet, for which purposes do you use it:

1. To communicate (e.g. by email)
2. Social networking
3. Online shopping
4. Information search
5. Internet banking
6. E-government services
7. I don't use the internet