

Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies

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

Noellie Brockdorff¹, Sandra Appleby-Arnold¹, Dušan Šoltés² ¹Department of Cognitive Science, University of Malta, Msida, Malta ²Univerzita Komenskeho v Bratislave, Slovakia

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

> The views expressed in this report are the sole responsibility of the authors and do not necessarily reflect the views of the European Union.

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	4
1.	Introduction	7
2.	Citizens' knowledge of surveillance	9
2.1	Awareness of different types of surveillance	9
2.2	Known reasons for surveillance	10
3.	Perceived usefulness and effectiveness of surveillance	10
3.1	Perceived usefulness	10
3.2	Effectiveness in protection against crime	12
3.3	Relationship between perceived usefulness and effectiveness	12
4.	Perceptions of surveillance	13
4.1	Surveillance and feelings of security	13
4.2	Personal information collected through surveillance	13
4.3	"Happiness" with surveillance	14
4.4	Relationship between security and happiness	14
4.5	Surveillance and privacy	15
4.6	Relationships between feelings, effectiveness of surveillance measures, and related laws	16
5.	Awareness of surveillance taking place	17
5.1	Noticing CCTV	17
5.2	Beliefs about surveillance taking place	17
6.	Acceptance of data sharing practices	18
7.	Acceptability of surveillance in different locations	20
8.	Economic costs of surveillance	21
9.	Social costs of surveillance	22
9.1	Attitudes towards surveillance	22
9.2	Behavioural changes resulting from surveillance	23
9.3	Perceived social benefits and social costs: Relationships	24
10.	Conclusion	25
Ap	pendices	26
Ap	pendix A: Figures and tables	27
Ap	pendix B: Questionnaire	42

0. Executive Summary

This document presents the results for Slovakia 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 Slovakia for age 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, face to face interviews were carried out during the same period. The Slovakia as their country of residence in the online survey or were administered the questionnaire face to face. The data collection was conducted by the local RESPECT project partner, the Comenius University in Bratislava (Faculty of Management), and in particular by its e-Europe Research & Development Centre, who also contributed to the questionnaire design, translations and back-translations.

Generally, the data reveal a rather large spread in the Slovakian respondents' knowledge of different types of surveillance and surveillance technologies, with surveillance using CCTV cameras (66%) being the type most respondents have heard of and the surveillance of data and traffic on the internet (26%) the least known. Many respondents also indicated that they know of a number of reasons for the setting up of surveillance, ranging between 57% for the detection of crime and 35% for the control of crowds. Most respondents think that surveillance is taking place in the country where they live, but one out of three respondents felt that they do not know about the economic costs of surveillance.

All types of surveillance being investigated (CCTV, surveillance using databases containing personal information, surveillance of online social networks, surveillance of financial transactions, and geolocation surveillance) were mostly perceived as more useful than not useful for the reduction, detection or prosecution of crime, with the highest mean score² for geolocation surveillance (3.71) for the prosecution of crime, and the lowest for surveillance using databases containing personal information (2.77) for the reduction of crime. Surveillance was perceived as being most useful for the prosecution of crime and least useful for the reduction of crime³. 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. Generally, though, 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.

¹ The total Slovakian sample consists of 352 respondents. However, due to the fact that responses were, at least partially, 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. The total sample for Slovakia will be fully included in the analyses for the synthesised all countries report (project deliverable D.11.3), which represents the overall results of this study.

² On a scale from 1 to 5, with 1=not useful at all, and 5=very useful.

³ With the exception of surveillance using databases containing personal information which was perceived most useful for the detection of crime.

The presence of surveillance makes the majority of Slovakian respondents feel insecure, and only in a very small number of respondents surveillance produces feelings of security.⁴ Regarding the respondents' feelings about personal information gathered through surveillance, they feel generally a strong lack of control over processing of personal information gathered via surveillance, irrespective of whether it has been gathered by 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 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 about all the different types of surveillance investigated, and they feel most unhappy about surveillance taking place without people knowing about it.

On the other side, the majority of Slovakian respondents disagreed more than agreed that the different types of surveillance have a negative impact on their privacy.⁵ CCTV is perceived to have the least negative impact on privacy. However, only very few respondents are willing to accept financial compensation in exchange for surveillance measures that would involve greater invasion of privacy (between 9% for CCTV surveillance and 14% for surveillance of financial transactions).

The sharing of information gathered through surveillance by government agencies with other government agencies, or with foreign governments is deemed acceptable by many 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 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".

Protection of the individual and, in particular, protection of the community were perceived as social benefits of surveillance. But risks ("social costs") associated with surveillance seemed to be more keenly felt. The highest risks were perceived to be the intentional misuse of information (mean score 6.17⁶) and misinterpretation (5.96) arising from surveillance, followed by privacy invasion and 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 concern, though not at the same level.

Few respondents have made changes to their behaviour as a result of being aware of surveillance. The change in behaviour that was reported most often (by 40% of respondents⁷) was stopping the exchange of personal data for discounts or vouchers, but less respondents have taken more proactive moves such as avoiding locations where surveillance is suspected to take place, filing complaints with the respective authorities, or taking defensive measures.

There were some significant gender differences in the findings. Female respondents had heard less than male respondents of most types and technologies of surveillance, but they showed some stronger beliefs in the

⁴ The remaining third felt neither secure not insecure or indicated "I don't know".

⁵ With the exception of surveillance using databases containing personal information, where an equal number of respondents agreed and disagreed.

⁶ On a scale from 1 to 7, with 1=disagree, and 7=agree.

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

usefulness of surveillance measures (in particular geolocation surveillance, surveillance of financial transactions and surveillance of online social networking). They also felt less insecure than male respondents in the presence of surveillance measures, and less unhappy about CCTV cameras, surveillance of online social networking and surveillance using databases containing personal information. On the other hand, there were no significant gender differences in the perceived effectiveness of surveillance, the awareness whether surveillance is taking place, the perception of social or economic costs, and feelings of control and trust related to the handling of personal data collected via surveillance measures.

To summarise, the Slovakian respondents indicated a strongly felt lack of trust in the protection of, and control over, personal information gathered via surveillance, they feel more unhappy than happy with the different types of surveillance, and they feel most unhappy about surveillance taking place without them knowing about it. At the same time, the majority of Slovakian respondents feel insecure in the presence of surveillance whilst only in a small minority surveillance produces feelings of security, but there is only a weak link between feeling happy, or unhappy, about surveillance and feeling secure or insecure through the presence of surveillance. However, analyses also indicate that increasing citizens' belief in the effectiveness of laws regarding the protection of personal data gathered via surveillance may make reduce citizens' feelings of insecurity more than only increasing the effectiveness of surveillance measures.

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 2012.⁸ 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. In Slovakia, this comprehensive data collection was conducted by the local RESPECT project partner, the Comenius University in Bratislava (Faculty of Management), and in particular by its e-Europe Research & Development Center, who also contributed to the questionnaire design, translations and back-translations.

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 2014.⁹ 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 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 Slovakian sample used for this analysis is based on the responses from 200 individuals who indicated Slovakia as their country of residence in the online survey or were administered the questionnaire face to face.¹⁰ The sample has a gender distribution of 52% females and 48% males, and an age distribution as see in figure 1 below which is representative for the Slovakian population.

⁸ Source: http://epp.eurostat.ec.europa.eu/portal/page/portal/population/data/main_tables.

⁹ The English version of this this questionnaire may be seen in Appendix B.

¹⁰ The total Slovakian sample consists of 352 respondents. However, due to the fact that responses were, at least partially, 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. The total sample for Slovakia will be fully included in the analyses for the synthesised all countries report (project deliverable D.11.3), which represents the overall results of this study.

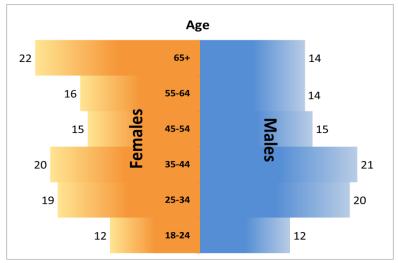


Figure 1: Age and gender distribution of Slovakian quota sample

Not fully satisfactory is the elevated level of education of the majority of respondents (56% with tertiary or postgraduate 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 is still more balanced than the education level of respondents in the total RESPECT sample (73%). Regarding specific demographic data related to aspects of surveillance, 35% of Slovakian respondents (16% of total sample) felt that they were living in an area with increased security risks, 23% (53% total sample) indicated that they usually travel abroad at least twice per year, and 29% (71% total sample) responded that they usually visited a mass event at least twice per year. Therefore, it can be assumed that a considerable proportion 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. Whilst the number of responses was, partially, too low in some groups¹¹ to allow for a full analysis by age that is statistically significant, gender aspects are discussed throughout all sections alongside the general results. For those questions where a sufficient number of responses were available in all age groups, age-related aspects will be discussed correspondingly. It has, however, to be kept in mind that, otherwise, results are only representative for the Slovakian population aged between 18 and 54 years.

¹¹ A substantial number of respondents in the age groups 65+ (80%-90%) and 55-64 (50%-70%) left most questions (except Q1, Q2, Q4, Q5.2.1, Q5.4 and Q6.2) unanswered.

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. A majority of Slovakian respondents indicated that they have heard of CCTV cameras (65.5%), whereas only a quarter (25.5%) had ever heard of the surveillance of data and traffic on the internet, such as Deep Packet and Deep Content Inspection. A split by gender shows some statistically significant differences. Male respondents indicated a greater awareness of surveillance using Global Positioning Systems than female respondents (difference between male and female responses: 18.8 percentage points), surveillance of data and traffic on the internet (difference 13.1 percentage points), surveillance of online communication (difference 13.2 percentage points), and CCTV cameras or surveillance of financial information (difference 10.2 percentage points). Regarding age, respondents of the 65+ years group had heard significantly less of all types and technologies of surveillance investigated (see Table A13 in Appendix A), whereas younger respondents had heard more than the others of the surveillance of "suspicious" behaviour (35-44 year olds), of surveillance of databases and online communication (25-34 year olds), and of surveillance of telecommunication (18-24 year olds).

Table 1
Knowledge of types of surveillance

		Answer = YES		ES
		Total	Female	Male
Q1_1	Biometric data , e.g. analysis of fingerprints, palm prints, facial or body features	52.5%	51.9%	53.1%
Q1_2	"Suspicious" behaviour , e.g. automated detection of raised voices, facial or body features	31.0%	31.7%	30.2%
Q1_3	Data and traffic on the internet, e.g. Deep Packet/Content inspection	25.5%	19.2%	32.3%*
Q1_4	Databases containing personal information, e.g. searching state pension databases, or customer databases of private companies	41.0%	43.3%	38.5%
Q1_5	Online communication , e.g. social network analysis, monitoring of chat rooms or forums	52.5%	46.2%	59.4%*
Q1_6	Telecommunication, e.g. monitoring of phone calls or SMS	61.0%	60.6%	61.5%
Q1_7	Electronic tagging / Radio Frequency Identification (RFID), e.g. tracking geolocation with electronic chips implanted under the skin or in bracelets	31.0%	27.9%	34.4%
Q1_8	Global Positioning Systems (GPS), e.g. tracking geolocation of cars or mobile phones	60.0%	51.0%	69.8%*
Q1_9	CCTV cameras, e.g. in public places, airports or supermarkets	65.5%	60.6%	70.8%*
Q1_10	Financial information, e.g. tracking of debit/credit card transactions	53.0%	48.1%	58.3%*

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

The reason for surveillance that is most known about is the detection of crime (56.5%), and the least known is the use of surveillance for control of crowds (34.5%). Respondents aged 65+ are less aware of detection of crime, prosecution of crime and control of border-crossings as main reasons for deploying surveillance, but there are no statistically significant gender differences, except for female respondents indicating more often than males that they don't know of any reasons.

Table 2 Known reasons for surveillance

		Answer=YES				
		Total	Female	Male		
Q2_1	The reduction of crime	50.0%	48.1%	52.1%		
Q2_2	The detection of crime	56.5%	54.8%	58.3%		
Q2_3	The prosecution of crime	52.0%	51.0%	53.1%		
Q2_4	Control of border-crossings	37.0%	34.6%	39.6%		
Q2_5	Control of crowds	34.5%	29.8%	39.6%		
Q2_6	Other	25.5%	22.1%	29.2%		
Q2_7	I don't know of any reasons.	7.5%	13.5%	1%*		

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

Geolocation surveillance is perceived as more useful for the reduction, detection, and prosecution of crime than the other four types of surveillance investigated, followed by CCTV and financial tracking. Surveillance of online social networking and surveillance using databases containing personal information were perceived to be the least useful. Four out of the five types of surveillance (CCTV, surveillance of online social networking, surveillance of financial transactions and geolocation surveillance) were perceived to be most useful for the detection of crime, slightly less useful for the prosecution of crime, and less useful still for the reduction of crime. In the case of surveillance using databases containing personal information, the usefulness for prosecution was rated marginally higher than for detection. Generally, though, all five types of surveillance investigated are perceived to be useful for the prosecution, and reduction of crime¹² (mean result in all categories is above the midpoint of 3.00 in Table 3).

There were some significant gender differences in the perception of usefulness of surveillance, with female respondents perceiving in particular geolocation surveillance, surveillance of online social networking and surveillance using databases containing personal information as more useful than male respondents for detection and prosecution of crime.

¹² With the exception of surveillance using databases containing personal information which was perceived as not useful by a majority of respondents for the purpose of reduction of crime.

Table 3Perceived usefulness of surveillance

		Total		Female		Male	
Q3.1	the reduction of crime	Mean	STD	Mean	STD	Mean	STD
Q3.1_1	CCTV cameras	3.13	1.495	3.30	1.450	2.96	1.530
Q3.1_2	Surveillance using databases containing personal information	2.77	1.353	3.00	1.439	2.57	1.250
Q3.1_3	Surveillance of online social networking	3.03	1.409	3.27	1.312	2.81	1.468
Q3.1_4	Surveillance of financial transactions	3.06	1.424	3.15	1.428	2.97	1.425
Q3.1_5	Geolocation surveillance	3.28	1.405	3.48	1.330	3.08	1.462
Q3.2	the detection of crime						
Q3.2_1	CCTV cameras	3.45	1.541	3.63	1.478	3.25	1.596
Q3.2_2	Surveillance using databases containing personal information	3.03	1.399	3.32	1.308	2.73*	1.436
Q3.2_3	Surveillance of online social networking	3.23	1.390	3.51	1.273	2.95*	1.453
Q3.2_4	Surveillance of financial transactions	3.45	1.392	3.77	1.320	3.14*	1.401
Q3.2_5	Geolocation surveillance	3.54	1.385	3.78	1.269	3.27*	1.462
Q3.3	the prosecution of crime						
Q3.3_1	CCTV cameras	3.29	1.539	3.48	1.510	3.08	1.556
Q3.3_2	Surveillance using databases containing personal information	3.14	1.486	3.24	1.465	3.04	1.513
Q3.3_3	Surveillance of online social networking	3.22	1.437	3.50	1.354	2.93*	1.474
Q3.3_4	Surveillance of financial transactions	3.45	1.414	3.71	1.385	3.17*	1.403
Q3.3_5	Geolocation surveillance	3.71	1.390	3.93	1.339	3.47	1.416

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 A3 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 CCTV surveillance 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 the other types of surveillance, with the relationship between perceived usefulness for prosecution of crime and perceived usefulness for detection of crime being typically the strongest. 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. Furthermore, strong relationships are observed between the different types of surveillance for the same purpose (with the exception of the relationship between CCTV and database surveillance for reduction of crime.

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 a pattern of results similar to 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 slightly less effective in protection against crime than they are deemed to be useful for the reduction, detection, and prosecution of crime. Between 45%¹³ (reduction of crime) and 54%¹⁴ (detection of crime) of respondents believed that CCTV is useful, but only 44%¹⁵ of respondents agreed that it is effective. CCTV is perceived as the most effective surveillance measure in protection against crime followed by geolocation surveillance and surveillance of financial transactions. Surveillance of online social-networking and surveillance using databases containing personal information are seen as the least effective methods of protection against crime. However, for all five types of surveillance respondents disagreed rather than agreed that they are an effective way to protect against crime. There were no gender differences found in these perceptions of effectiveness.

Perceived effectiveness of surveillance Total Female Male STD Mean Mean STD Mean STD CCTV is an effective way to protect against Q5.1.1_1 3.81 2.109 4.01 2.024 3.61 2.187 crime Surveillance utilising databases containing Q5.1.1 2 3.11 1.775 3.11 1.769 3.12 1.797 personal information is an effective way to protect against crime Surveillance of online social-networking is an Q5.1.1_3 3.31 1.848 3.40 1.784 3.21 1.925 effective way to protect against crime Surveillance of financial transactions is an Q5.1.1_4 3.70 1.922 3.86 1.853 3.52 1.991 effective way to protect against crime Geolocation surveillance is an effective way to 3.96 2.004 Q5.1.1_5 3.78 2.062 2.112 3.58 protect against crime.

 Table 4

 Perceived effectiveness of surveillance

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.

3.3 Relationship between perceived usefulness and effectiveness

There is a visible 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) – in particular for CCTV and geolocation surveillance. The strongest relationships, here, are found for the relationships between effectiveness in the protection against crime and usefulness for the reduction of crime.

¹³ Answers 4 or 5 on a scale from 1 to 5, with 1=not useful at all and 5=very useful.

¹⁴ Answers 4 or 5 on a scale from 1 to 5, with 1=not useful at all and 5=very useful.

¹⁵ Answers 5, 6 or 7 on a scale from 1 to 7, with 1=disagree and 7=agree.

4. Perceptions of surveillance

4.1 Surveillance and feelings of security

As seen in the previous section, most of the different types of surveillance are perceived as useful in the reduction, detection, and prosecution of crime, but not as particularly effective in the protection against crime. At the same time, the presence of surveillance does not appear to produce strong feelings of security in many respondents. The mean result – with female respondents feeling less insecure than males – is clearly below the midpoint of 3.00 on a five-point scale (see Table 5 in next section). For more than two thirds of respondents (71%), the presence of surveillance makes them feel insecure (1 or 2 on a 5-point scale, with 1=very insecure and 5=very secure), whereas only a very small number of respondents (6%) feel secure (4 or 5 on a 5-point scale, with 1=very insecure and 5=very secure) when surveillance is present. Inbetween age groups, respondents aged 65+ feel the most insecure, and significantly more insecure than younger respondents, in particular those aged 25-34 (see Table A15 in Appendix A).

4.2 Personal information collected through surveillance

Respondents, and male respondents even more than females, generally feel a 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. Regarding data gathered by government agencies, respondents aged 35-44 feel themselves to be significantly more in control than those aged 45-54 and 65+, whereas for data gathered by private companies it is the youngest respondents (18-24 years) who feel more in control than the older ones (see Table A15 in Appendix A). There is also a visible lack of trust in both private companies and government agencies being able to protect personal information gathered via surveillance with, again, older respondents feeling significantly more mistrust than many younger respondents. 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.

		Total		Female		Ma	ale
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	1.95	1.008	2.14	1.066	1.75*	0.907
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? How much control do you think you have over the	1.67	1.033	1.86	1.135	1.48*	0.885
4.4.2	processing of personal information gathered by private companies via surveillance measures?	1.72	1.073	1.82	1.160	1.62	0.972
4.5	Trust (1=no trust; 5=complete trust)						
4.5.1	How much do you trust <u>government agencies</u> that they protect your personal information gathered via surveillance measures?	1.79	1.054	1.99	1.163	1.58*	0.889

Table 5Feelings of security, control and trust

How much do you trust <u>private companies</u> that 4.5.2 they protect your personal information gathered 1.71 0.957 1 via surveillance measures?

1.71	0.957	1.85	1.061	1.56*	0.817

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 all the different types of surveillance investigated, with males feeling significantly more unhappy than females¹⁶. They appear to feel most unhappy with surveillance using databases containing personal information (mean score 3.64), and they are unhappier still with surveillance taking place without people knowing about it (mean score 4.03). Regarding the latter, the oldest respondents (65+ year olds) feel significantly more unhappy than the youngest (18-24 year olds; see Table A16 in Appendix A).

Happiness with surveillance							
		То	tal	Female		Ma	ale
		Mean	STD	Mean	STD	Mean	STD
5.3_1	Feel happy/unhappy about CCTV cameras	3.42	1.176	3.19	1.118	3.65*	1.196
5.3_2	Feel happy/unhappy about surveillance of online social networks	3.49	1.055	3.21	0.957	3.78*	1.085
5.3_3	Feel happy/unhappy about surveillance using databases	3.64	0.976	3.43	0.944	3.89*	0.961
5.3_4	Feel happy/unhappy about surveillance of financial transactions	3.36	1.026	3.31	0.990	3.40	1.069
5.3_5	Feel happy/unhappy about geolocation surveillance	3.37	1.014	3.19	0.930	3.56	1.072
5.4	Feel happy/unhappy about surveillance taking place without noticing	4.03	1.010	4.03	1.052	4.03	0.973

Table 6 Happiness with surveillance

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.

4.4 Relationship between security and happiness

There are some 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 happy or unhappy with social-networking surveillance. And those who are happy or unhappy with geolocation surveillance have similar feelings about all other types of surveillance. There is also a 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, but it is much weaker. This means that being happy or unhappy with different types of surveillance – which could be assumed to be due to their "technical" visibility or invisibility – cannot be simply related to people being aware whether surveillance is taking place. Being happy or unhappy with different types of surveillance is only weakly related to

¹⁶ For CCTV cameras, surveillance of online social networks, and surveillance using databases containing personal information.

feelings of security as a consequence of the presence of surveillance. Furthermore, being happy or unhappy with all types of surveillance (except CCTV) is only weakly linked to the perceived usefulness of the respective type of surveillance for reduction, detection and prosecution of crimes (see table A2 in Appendix A).

4.5 Surveillance and privacy

Table 7							
	Perceptio	ns of priv	асу				
		То	tal	Fem	ale	Ma	ale
5.1.2	Privacy (1=disagree; 7=agree)	Mean	STD	Mean	STD	Mean	STD
5.1.2_1	CCTV has a negative impact on one's privacy	3.18	2.183	3.10	2.055	3.28	2.332
5.1.2_2	Surveillance via databases has a negative impact on one's privacy	4.00	2.182	3.69	2.113	4.35	2.224
5.1.2_3	Surveillance of online social networks has a negative impact on one's privacy	3.88	2.124	3.69	1.959	4.09	2.293
5.1.2_4	Surveillance of financial transactions has a negative impact on one's privacy	3.69	2.076	3.55	1.967	3.86	2.207
5.1.2_5	Geolocation surveillance has a negative impact on one's privacy	3.88	2.132	3.71	2.074	4.07	2.199

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, both female and male, disagreed more than agreed that the different types of surveillance have a negative impact on one's privacy (Table 7). Only for surveillance using databases containing personal information an equal number of respondents agreed and disagreed that there is a negative impact (mean score 4.0, i.e. at the mid-point of the scale from 1 to 7). CCTV is perceived to have the least negative impact on privacy. Irrespective of their views on the impact of different types of surveillance on privacy, very few respondents are willing to accept financial compensation in exchange for surveillance measures that would involve greater invasion of privacy (Table 8). There is, mostly, no significant gender difference in the acceptance of such a trade between financial compensation and increased intrusion on their privacy, with the exception of male respondents being more willing to accept financial compensation for privacy invasion through surveillance of financial transactions.

Table 8 Financial privacy trade-off

5.1.3	Would you be willing to accept payment as compensation for greater	Answer=YES				
	invasion of your privacy, using:	Total	Female	Male		
5.1.3_1	Surveillance via CCTV cameras	8.6%	2.6%	14.3%		
5.1.3_2	Surveillance of online social networks	12.3%	10.3%	14.3%		
5.1.3_3	Surveillance utilising databases containing personal information	9.9%	10.3%	9.5%		
5.1.3_4	Surveillance of financial transactions	13.6%	10.3%	16.7%*		
5.1.3_5	Geolocation surveillance	12.3%	12.8%	11.9%		

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 not related to their perceived impact of surveillance on privacy (see table A10 in Appendix A). Perceived impact of surveillance on privacy was also not related with feelings of trust in private companies and government agencies being able to protect personal information gathered via surveillance, or to 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 perceived moderate negative impact of surveillance on one's privacy, these feelings appear not to be necessarily related.

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

There are moderate relationships between the respondents feeling secure due to the presence of surveillance, and feelings of control over their personal data collected through surveillance. However, there is a strong link between control over one's personal data collected by government agencies through surveillance and trust that personal data gathered by government agencies through surveillance is protected; an even stronger connection can be found between control over one's personal data collected by private companies through surveillance and trust that personal data gathered by private companies through surveillance is protected (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 only marginally stronger than the relationship with feelings of trust that personal data gathered by private companies is protected. There is a similar pattern between the relationship between the perceived effectiveness of data protection laws and control over personal data collected through surveillance by government agencies and private companies. These findings may be due to the fact that data protection laws are perceived as being applied by or being applicable to government agencies not significantly more than to private companies. However, there is a rather strong relationship between the perceived effectiveness of 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 increase in feelings of security in the presence of surveillance.

There are much weaker relationships between perceived effectiveness of different surveillance measures and feelings of security in the presence of surveillance (see table A12 Appendix A). This suggests that increasing the perceived effectiveness of surveillance itself may not have the same effect as increasing citizens' belief in the effectiveness of data protection laws related to surveillance.

5. Awareness of surveillance taking place

5.1 Noticing CCTV

whether CCTV is noticed					
Q5.2.1	Total	Female	Male		
I never notice CCTV cameras.	7.5%	9.6%	5.2%		
I rarely notice CCTV cameras.	23.0%	24.0%	21.9%		
I sometimes notice CCTV cameras.	30.0%	30.8%	29.2%		
I often notice CCTV cameras.	25.0%	21.2%	29.2%		
I always notice CCTV cameras.	10.5%	9.6%	11.5%		
I don't know / No answer	4.0%	4.8%	3.1%		

Table 9 Whether CCTV is noticed

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.

Overall, only 35.5% of respondents often or always notice CCTV cameras, whilst 30.5% of respondents rarely or never notice CCTV cameras. There is no statistically significant gender difference in whether CCTV I noticed, but some age-related differences. Respondents aged between 18 and 34 indicated significantly more often that the others that they rarely notice CCTV cameras, whereas those aged 55-64 indicated most often that they always notice CCTV (see Table A17 in Appendix A).

5.2 Beliefs about surveillance taking place

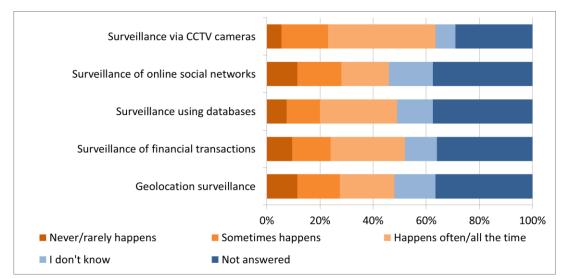


Figure 2: Q5.2.2 – In your opinion, how often do the following types of surveillance take place in the country where you live?

Although almost all respondents indicated whether or not they notice CCTV cameras in their daily lives (see previous Table 9), a rather large proportion of them did not reveal their beliefs how often surveillance actually takes place in the country where they live. In particular, the 55-64 year olds (50-60%) and the 65+ year olds (80-90%) left this question unanswered. Of the remaining respondents, 41% believe that CCTV surveillance takes place often or all the time in the country where they live. Fewer respondents believe that the other types of surveillance take place, between 19% and 21% for surveillance of online social-networking, surveillance using databases containing

personal information, surveillance of financial transactions and geolocation surveillance. There are, again, no significant differences between male and female responses.

6. Acceptability of data sharing practices

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	4.5%	2.0%	0.0%				
Acceptable only if the citizen is suspected of wrong-doing	14.5%	14.0%	9.0%				
Acceptable only if the citizen is suspected of wrong-doing an the surveillance is legally authorised	23.5%	23.5%	16.0%				
Acceptable if the citizen is informed	12.5%	11.5%	9.0%				
Acceptable if the citizen has given consent	15.5%	12.0%	21.5%				
Not acceptable in any circumstances	12.0%	13.0%	21.5%				
l don't know	8.5%	8.5%	8.5%				

Table 10

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 many 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. Only about one out of eight participants believes it is acceptable for information gathered through surveillance by government agencies to be shared if the citizen has given consent. Whilst results regarding the sharing of information with other government agencies or foreign governments are mostly fairly similar, sharing information with private companies is less acceptable even if surveillance has been lawfully authorised for somebody suspected of wrong-doing. A considerable minority of respondents (21.5%) think it is unacceptable in all circumstances 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	2.5%	2.0%	0,5%
Acceptable only if the citizen is suspected of wrong-doing	9.0%	8.0%	8.5%
Acceptable only if the citizen is suspected of wrong-doing an the surveillance is legally authorised	15.0%	17.0%	9.5%
Acceptable if the citizen is informed	12.0%	9.5%	8.0%
Acceptable if the citizen has given consent	21.0%	20.5%	23.0%
Not acceptable in any circumstances	19.0%	21.0%	24.5%
I don't know	7.5%	7.5%	7.5%

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) for private companies to share a citizen's personal information. Lawfulness still has a strong effect, but it is slightly 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 it is deemed unacceptable in any circumstances for private companies to share citizen's personal information with other private companies (24.5%).

7. Acceptability of surveillance in different locations

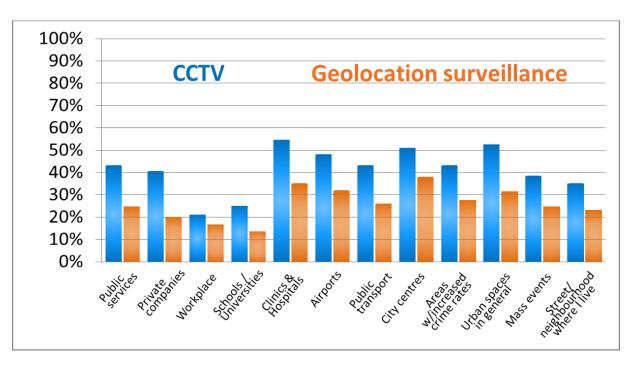


Figure 3: Acceptability of surveillance in different locations Q6.1 – In which of the following locations or events would you find the different types of surveillance for fighting crime acceptable?

CCTV surveillance is perceived as clearly more acceptable than geolocation surveillance for the purposes of fighting crime in all the events and locations. Acceptance rates for CCTV are between 25% and 100% higher than those for geolocation surveillance. CCTV is least accepted in the workplace (21%), geolocation surveillance finds the least acceptance in schools and universities (13.5%). The highest acceptance of surveillance by CCTV is in clinics and hospitals (54.5%), urban spaces in general (52.5%) and city centres (51%). A possible explanation for this rather surprising result could be that such comparatively elevated acceptance levels of surveillance in clinics and hospitals may be related to higher 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 all other locations is below the 50% mark; geolocation surveillance is, generally, accepted only by a minority of respondents in all locations. Except for female respondents finding workplace surveillance via CCTV cameras more acceptable than males, there are no statistically significant gender differences.

8. Economic costs of surveillance

Only about one in eight 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"; 19.5% indicated that, in their opinion, there was too little or far too little money allocated, 31.5% believed it was too much or far too much, and in particular participants aged 65+ feel more than respondents of all other ages that there is far too much spent (see table A18 in Appendix A). But overall one out of every three respondents felt that they, actually, "don't know" whether government agencies are allocated sufficient funds for carrying out surveillance for the purpose of fighting crime. 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 one out of every five of these respondents indicated they would be willing to do so whilst almost four times as many replied that they would not, with no statistically significant gender difference.¹⁷

	Table :	12							
Beliefs about money allocated to surveillance Total Female Male far too little 7.0% 6.7% 7.3% too little 12.5% 12.5% 12.5% just right 15.0% 20.2% 9.4% too much 11.0% 7.7% 14.6%									
	Total		Female	Male					
far too little	7.0%		6.7%	7.3%					
too little	12.5%		12.5%	12.5%					
just right	15.0%		20.2%	9.4%					
too much	11.0%		7.7%	14.6%					
far too much	20.5%		17.3%	24.0%					
I don't know	33.0%		35.6%	30.2%					
No answer	1.0%		0.0%	2.1%					

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

	Total	Female	Male
Yes	17.9%	20.0%	15.8%
No	66.7%	60.0%	73.7%
I don't know	5.1%	10.0%	0.0%
No answer	10.3%	10.0%	10.5%

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.

¹⁷ However, the comparatively low number of respondents to this question (n=39) allows only very cautious interpretations.

9. Social costs of surveillance

9.1 Attitudes towards surveillance

On one hand, protection of the individual citizen and, in particular, protection of the community were perceived as the social benefits of surveillance. But, on the other hand, most risks associated with surveillance seemed to be more keenly felt. The highest perceived risk is that information gathered through surveillance is intentionally misused, followed by the risk of misinterpretation, privacy invasion through surveillance, and that surveillance may violate citizens' right to control whether information about them is used. The risk that surveillance may limit a citizen's right of expression and free speech also appears to be an issue, though not at the level of data misuse and data misinterpretation. There are no significant gender differences in the perceptions of social benefits and costs of surveillance.

		To	tal	Fem	ale	Ma	ale
		Mean	STD	Mean	STD	Mean	STD
Q8.1.1	Surveillance provides protection to the individual citizen	4.21	1.845	4.36	1.823	4.04	1.873
Q8.1.2	Surveillance provides protection of the community	4.47	1.786	4.49	1.722	4.45	1.880
Q8.1.3	Surveillance can be a source of personal excitement	4.53	2.072	4.42	2.195	4.65	1.946
Q8.1.4	Surveillance can be something to play with	5.40	1.889	5.37	1.918	5.44	1.873
Q8.1.5	Surveillance may cause discrimination towards specific groups of society	4.44	2.160	4.47	2.192	4.40	2.144
Q8.1.6	Surveillance may be a source of stigma	4.60	1.954	4.35	2.057	4.90	1.805
Q8.1.7	Surveillance may violate a person's privacy	5.72	1.780	5.68	1.812	5.78	1.755
Q8.1.8	Surveillance may violate citizens' right to control whether information about them is used	5.42	1.730	5.34	1.692	5.51	1.783
Q8.1.9	There is a potential that information gathered via surveillance could be intentionally misused	6.17	1.412	6.20	1.347	6.14	1.493
Q8.1.10	There is a potential that information gathered via surveillance could be misinterpreted	5.96	1.447	6.08	1.359	5.82	1.541
Q8.1.11	Surveillance may limit a citizen's right of expression and free speech	5.37	1.938	5.41	1.839	5.34	2.048
Q8.1.12	Surveillance may limit a citizen's right of communication	4.82	2.019	4.93	1.990	4.71	2.061

Table 14Attitudes towards surveillance

Q8.1.13 Surveillance may limit a citizen's right of information	4.80	1.972	4.79	1.872	4.82	2.106
---	------	-------	------	-------	------	-------

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

Rather few respondents have made changes to their behaviour as a result of being aware of surveillance. The change in behaviour that was undertaken most often (by 40% of respondents¹⁸) was to stop exchanging personal data for discounts or vouchers, but less respondents have taken more proactive moves such as avoiding locations where surveillance is suspected to take place, filing complaints with the respective authorities, or taking defensive measures.

		То	tal	Fem	nale	Male		
		Mean	STD	Mean	STD	Mean	STD	
Q8.2.1	I have restricted my activities or the way I behave	3.64	2.207	3.64	2.214	3.64	2.220	
Q8.2.2	I have avoided locations or activities where I suspect surveillance is taking place	3.30	2.255	3.38	2.285	3.22	2.242	
Q8.2.3	I have taken defensive measures (hiding face, faking data, incapacitating surveillance device)	2.79	2.137	2.46	1.988	3.13	2.249	
Q8.2.4	I have made fun of it	2.43	1.956	2.32	1.917	2.54	2.007	
Q8.2.5	I have filed a complaint with the respective authorities	2.30	1.957	2.23	1.945	2.38	1.989	
Q8.2.6	I have informed the media	2.21	1.918	2.33	2.082	2.08	1.724	
Q8.2.7	I have promoted or participated in collective actions of counter- surveillance	2.51	2.020	2.20	1.947	2.85	2.062	
Q8.2.8	have kept myself informed about technical possibilities to protect my personal data	3.66	2.123	3.51	2.122	3.84	2.132	
Q8.2.9	I have stopped accepting discounts or vouchers if they are in exchange for my personal data	4.27	2.312	4.12	2.388	4.45	2.221	

Table 15Behaviour changes resulting from an awareness of surveillance

¹⁸ Answers 5, 6 and 7 on a scale from 1 to 7, with 1=disagree and 7=agree.

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 moderately related to each other, i.e. a number of respondents have the same beliefs about both these benefits. However, these perceived benefits appear to be largely independent of the perceived social costs.

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 right of free speech and the right of communication;
- surveillance limiting the right of information and being a potential source of stigma;
- the potential for surveillance to violate privacy and the right of citizens to control whether information collected about them through surveillance is used; and
- surveillance being a potential source of discrimination and limiting citizens' right of communication (see Table A3 in Appendix A).

Generally, it appears that respondents do perceive both social costs and benefits, but without necessarily "weighing" them against each other. Additionally, there is only a very weak 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).

There are some moderate to strong links between changes in different behaviours as a result of awareness of surveillance. The strongest connections are between filing complaints, informing the media, promoting or participating in collective actions of counter-surveillance, and taking defensive measures (see Table A4 in Appendix A). These can be seen to represent certain "strategies" of protection against surveillance, though it needs to be kept in mind that only a minority respondents have acted in this way (see Table 15 above). The change of personal behaviour most often indicated by respondents – not accepting discounts/vouchers in exchange for personal data – is only weakly to moderately related to the other forms of behavioural changes (see Table A4 in Appendix A).

With, generally, only weak or very weak links, there is little evidence in this study 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 and data misinterpretation – appear mostly not to be linked at all to any of the behavioural changes investigated.

10. Conclusion

Overall, the Slovakian respondents 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 Slovakian respondents feel more unhappy than happy with the different types of surveillance, and they feel most unhappy about surveillance taking place without them knowing about it. At the same time, the majority of Slovakian respondents feel insecure in the presence of surveillance whilst only in a small minority surveillance produces feelings of security, but there is only a weak link between feeling happy, or unhappy, about surveillance and feeling secure or insecure through the presence of surveillance.

However, analyses also indicate that increasing citizens' belief in the effectiveness of laws regarding the protection of personal data gathered via surveillance may make reduce citizens' feelings of insecurity more than only increasing the effectiveness of surveillance measures.

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

Figure 1: Age and gender distribution of UK quota sample

Figure 2: Beliefs about surveillance taking place

Figure 3: Acceptability of surveillance in different locations

Table 1: Knowledge of types of surveillance Table 2: Known reasons of surveillance Table 3: Perceived usefulness of surveillance Table 4: Perceived effectiveness of surveillance Table 5: Feelings of security, control and trust Table 6: Happiness with surveillance Table 7: Perceptions of privacy Table 8: Financial privacy trade-off Table 9: Noticing CCTV Table 10: Acceptability of data sharing practices of government agencies Table 11: Acceptability of data sharing practices of private companies Table 12: Beliefs about money allocated to surveillance Table 13: Willingness to pay more taxes to increase budget allocated to carry out surveillance to fight crime Table 14: Attitudes towards surveillance Table 15: Behaviour changes resulting from an awareness of surveillance Table A1: Correlations – Usefulness for reduction, detection and prosecution of crime Table A2: Correlations – Usefulness and happiness / feeling of security Table A3: Correlations – Social costs (perceptions)

Table A4: Correlations – Social costs (behaviour)

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

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

Table A7: Correlations – Social costs and privacy in surveillance

Table A8: Correlations – Usefulness vs. effectiveness of surveillance

Table A9: Correlations – Security and happiness

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

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

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

Table A13: Knowledge of types of surveillance by age group

Table A14: Known reasons for surveillance by age group

Table A15: Feelings of security, control and trust by age group

Table A16: Happiness with surveillance by age group

Table A17: Awareness of CCTV by age group

Table A18: Beliefs about economic costs of surveillance by age group

				Usefulness f	or REDUC	FION of crim	e
			CCTV	database	SNS	financialT	geolocat.
			Q3.1_1	Q3.1_2	Q3.1_3	Q3.1_4	Q3.1_5
z	CCTV	Q3.1_1	1.000	0.359	0.541	0.487	0.539
<u>I</u> OI	database	Q3.1_2	0.359	1.000	0.671	0.611	0.676
ы С	SNS	Q3.1_3	0.541	0.671	1.000	0.576	0.716
REDUCTION	financT	Q3.1_4	0.487	0.611	0.576	1.000	0.654
œ	Geoloc.	Q3.1_5	0.539	0.676	0.716	0.654	1.000
7	CCTV	Q3.2_1	0.791	0.460	0.508	0.535	0.505
DETECTION	database	Q3.2_2	0.364	0.717	0.567	0.473	0.638
ECT	SNS	Q3.2_3	0.474	0.513	0.706	0.522	0.642
DET	financT	Q3.2_4	0.551	0.508	0.584	0.634	0.590
-	Geoloc.	Q3.2_5	0.574	0.569	0.648	0.510	0.752
Z	CCTV	Q3.3_1	0.695	0.403	0.459	0.597	0.509
Ĕ	database	Q3.3_2	0.423	0.705	0.493	0.636	0.613
EC	SNS	Q3.3_3	0.383	0.596	0.613	0.535	0.629
PROSECUTION	financT	Q3.3_4	0.500	0.536	0.482	0.613	0.579
РН	Geoloc.	Q3.3_5	0.581	0.517	0.552	0.606	0.647

Usefulness for **DETECTION** of crime

			CCTV Q3.2_1	database Q3.2_2	SNS Q3.2_3	financialT Q3.2_4	geolocat. Q3.2_5
7	ССТV	Q3.2_1	1.000	0.502	0.593	0.714	0.724
õ	database	Q3.2_2	0.502	1.000	0.713	0.564	0.678
DETECTION	SNS	Q3.2_3	0.593	0.713	1.000	0.610	0.747
Ĕ	financT	Q3.2_4	0.714	0.564	0.610	1.000	0.701
•	Geoloc.	Q3.2_5	0.724	0.678	0.747	0.701	1.000
Z	CCTV	Q3.3_1	0.791	0.454	0.575	0.608	0.561
PROSECUTION	database	Q3.3_2	0.558	0.708	0.547	0.553	0.546
ECL	SNS	Q3.3_3	0.535	0.644	0.732	0.546	0.600
sos	financT	Q3.3_4	0.685	0.461	0.536	0.731	0.634
РБ	Geoloc.	Q3.3_5	0.722	0.515	0.601	0.630	0.698

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
Z	CCTV	Q3.3_1	1.000	0.610	0.607	0.690	0.783
PROSECUTION	database	Q3.3_2	0.610	1.000	0.751	0.722	0.652
EC	SNS	Q3.3_3	0.607	0.751	1.000	0.675	0.646
SOS	financT	Q3.3_4	0.690	0.722	0.675	1.000	0.760
РЕ	Geoloc.	Q3.3_5	0.783	0.652	0.646	0.760	1.000

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

				HAPPINES	S with su	Feeling of		
			CCTV	CCTV Database SNS Fina		FinancT	Geoloc.	SECURITY
			Q5.3_1	Q5.3_3	Q5.3_2	Q5.3_4	Q5.3_5	 Q4.3
N	CCTV	Q3.1_1	-0.579	-0.313	-0.304	-0.323	-0.363	0.499
	database	Q3.1_2	-0.174	-0.219	-0.246	-0.182	-0.241	0.288
ulness UCTIO crime	SNS	Q3.1_3	-0.338	-0.356	-0.195	-0.309	-0.427	0.277
Usefulness fo REDUCTION of crime	financialT	Q3.1_4	-0.235	-0.233	-0.258	-0.314	-0.244	0.262
Ĵ E	geolocat.	Q3.1_5	-0.264	-0.293	-0.255	-0.322	-0.379	0.29
z fo	CCTV	Q3.2_1	-0.621	-0.219	-0.279	-0.367	-0.362	0.462
	database	Q3.2_2	-0.215	-0.301	-0.299	-0.222	-0.332	0.203
Usefulness fo DETECTION of crime	SNS	Q3.2_3	-0.248	-0.247	-0.211	-0.304	-0.297	0.191
sefu DET of	financialT	Q3.2_4	-0.319	-0.283	-0.250	-0.353	-0.278	0.319
Š 🖬	geolocat.	Q3.2_5	-0.333	-0.317	-0.313	-0.420	-0.487	0.285
for ON	CCTV	Q3.3_1	-0.487	-0.248	-0.244	-0.326	-0.349	0.434
ne fiss f	database	Q3.3_2	-0.215	-0.285	-0.183	-0.158	-0.283	0.318
ulness ECUTI crime	SNS	Q3.3_3	-0.181	-0.238	-0.140	-0.238	-0.322	0.257
Usefulness for PROSECUTION of crime	financialT	Q3.3_4	-0.305	-0.281	-0.237	-0.287	-0.382	0.271
j⊃ H	geolocat.	Q3.3_5	-0.416	-0.260	-0.264	-0.331	-0.453	0.255

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	0.456	1.000											
Source of excitement	Q8.1_3	-0.032	-0.015	1.000										
Something to play with	Q8.1_4	0.049	0.081	0.249	1.000									
Cause of discrimi- nation	Q8.1_5	-0.174	-0.074	0.501	0.301	1.000								
Source of stigma	Q8.1_6	0.095	0.112	0.435	0.371	0.406	1.000							
Violates privacy	Q8.1_7	-0.167	0.120	0.360	0.320	0.473	0.243	1.000						
Violates right of control data	Q8.1_8	0.025	0.107	0.590	0.199	0.391	0.319	0.618	1.000					
Potential misuse	Q8.1_9	0.022	0.244	0.154	0.413	0.202	0.305	0.494	0.273	1.000				
Potential mis- interpre- tation	Q8.1_10	0.054	0.132	0.280	0.318	0.304	0.304	0.368	0.325	0.556	1.000			
Limits right of free speech	Q8.1_11	-0.049	0.019	0.521	0.310	0.469	0.277	0.588	0.544	0.362	0.376	1.000		
Limits right of communi- cation	Q8.1_12	0.012	0.179	0.369	0.257	0.600	0.511	0.535	0.549	0.261	0.199	0.647	1.000	
Limits right of information	Q8.1_13	-0.063	0.048	0.377	0.294	0.543	0.620	0.397	0.506	0.300	0.256	0.447	0.553	1.000

Table A4: Correlations – Social costs (behaviour)

Social costs II (behaviour)		restrict- ed activities	avoided locations	defen- sive measures	made fun of it	filed com- plaint	in- formed the media	counter- sur- veillance	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	0.615	1.000							
defensive measures	Q8.2_3	0.416	0.578	1.000						
made fun of it	Q8.2_4	0.165	0.263	0.462	1.000					
filed complaint	Q8.2_5	0.461	0.602	0.682	0.542	1.000				
informed the media	Q8.2_6	0.375	0.481	0.665	0.666	0.872	1.000			
counter-surveillance	Q8.2_7	0.444	0.525	0.756	0.462	0.814	0.775	1.000		
info about technical protection	Q8.2_8	0.449	0.521	0.584	0.293	0.404	0.299	0.550	1.000	
stopped accepting vouchers	Q8.2_9	0.509	0.493	0.473	0.194	0.368	0.271	0.353	0.417	1.000

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

Social costs III (perceptions vs behaviour)		restrict- ed activities	avoided locations	defen- sive measures	made fun of it	filed com- plaint	in- formed the media	counter- sur- veillance	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	-0.076	0.051	-0.081	-0.108	0.206	0.233	0.049	-0.024	-0.001
Protection of community	Q8.1_2	-0.165	-0.195	-0.297	-0.036	-0.169	-0.046	-0.229	-0.131	-0.089
Source of excitement	Q8.1_3	0.172	0.099	0.131	0.066	0.090	-0.061	0.025	0.326	0.157
Something to play with	Q8.1_4	-0.090	0.005	-0.012	-0.211	-0.136	-0.213	-0.061	0.051	0.010
Cause of discrimination	Q8.1_5	0.206	0.253	0.133	0.127	0.182	0.099	0.143	0.297	0.227
Source of stigma	Q8.1_6	-0.058	0.036	0.019	0.146	0.075	0.019	0.153	0.103	0.192
Violates privacy	Q8.1_7	0.204	0.212	0.110	0.073	-0.131	-0.147	0.009	0.307	0.263
Violates right to control data	Q8.1_8	0.169	0.099	0.107	0.131	0.094	0.003	0.143	0.374	0.249
Potential misuse	Q8.1_9	0.001	-0.039	-0.254	-0.228	-0.412	-0.495	-0.315	0.011	0.135
Potential misinterpretation	Q8.1_10	0.033	0.035	-0.105	-0.302	-0.232	-0.329	-0.175	0.116	0.139
Limits right of free speech	Q8.1_11	0.243	0.256	0.168	-0.109	0.109	0.000	0.137	0.347	0.247
Limits right of communi cation	Q8.1_12	0.120	0.135	-0.023	0.007	0.049	-0.006	0.125	0.226	0.245
Limits right of information	Q8.1_13	0.038	0.163	-0.030	0.169	0.064	-0.011	0.049	0.105	0.129

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

			individual citizen	community
			Q8.1_1	Q8.1_2
	CCTV	Q3.1_1	0.245	0.290
Usefulness for	Database	Q3.1_2	0.137	0.128
REDUCTION of	SNS	Q3.1_3	0.161	0.166
crime	financialT	Q3.1_4	0.230	0.182
	geolocat.	Q3.1_5	0.164	0.192
	CCTV	Q3.2_1	0.188	0.277
Usefulness for	Database	Q3.2_2	0.021	0.099
DETECTION of	SNS	Q3.2_3	0.046	0.143
crime	financialT	Q3.2_4	0.109	0.167
	geolocat.	Q3.2_5	0.074	0.110
	CCTV	Q3.3_1	0.242	0.284
Usefulness for	Database	Q3.3_2	0.259	0.076
PROSECUTION	SNS	Q3.3_3	0.231	0.123
of crime	financialT	Q3.3_4	0.224	0.008
	geolocat.	Q3.3_5	0.261	0.147
		05444	0.070	0.000
	CCTV	Q5.1.1_1	0.278	0.339
	Database	Q5.1.1_2	0.196	0.195
EFFECTIVENESS	SNS	Q5.1.1_3	0.182	0.246
	financialT	Q5.1.1_4	0.170	0.225
	geolocat.	Q5.1.1_5	0.274	0.297

		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	-0.137	-0.271	-0.203	-0.269	-0.334			
Q8.1_2	Protection of community	-0.086	-0.132	-0.079	-0.147	-0.174			
Q8.1_3	Source of excitement	0.156	0.429	0.309	0.481	0.358			
Q8.1_4	Something to play with	0.116	0.198	0.070	0.198	0.082			
Q8.1_5	Cause of discrimination	0.285	0.416	0.372	0.495	0.388			
Q8.1_6	Source of stigma	0.197	0.252	0.206	0.342	0.191			
Q8.1_7	Violates privacy	0.196	0.424	0.378	0.365	0.386			
Q8.1_8	Violates right of control data	0.140	0.416	0.375	0.364	0.339			
Q8.1_9	Potential misuse	-0.043	0.151	0.100	0.075	0.084			
Q8.1_10	Potential misinterpretation	0.080	0.117	0.098	0.079	0.064			
Q8.1_11	Limits right of free speech	0.215	0.377	0.347	0.416	0.445			
Q8.1_12	Limits right of communication	0.235	0.412	0.380	0.473	0.428			
Q8.1_13	Limits right of information	0.194	0.317	0.297	0.376	0.345			
	Social costs (behaviour)								
Q8.2_1	restricted activities	0.155	0.165	0.123	0.121	0.203			
Q8.2_2	avoided locations	0.191	0.158	0.072	0.252	0.221			
Q8.2_3	defensive measures	0.180	0.110	0.078	0.131	0.190			
Q8.2_4	made fun of it	0.257	0.161	0.250	0.180	0.183			
Q8.2_5	filed complaint	0.186	0.056	0.048	0.107	0.151			
Q8.2_6	informed the media	0.106	-0.083	-0.013	0.001	0.021			
Q8.2_7	counter-surveillance	0.262	0.120	0.171	0.197	0.251			
Q8.2_8	info about technical protection	0.284	0.386	0.291	0.307	0.330			
Q8.2_9	stopped accepting vouchers	0.092	0.218	0.212	0.158	0.218			

Surveillance measures having a negative impact on privacy

Table A8: Correlations – Usefulness vs. effectiveness of surveillance

				EFFECTIVE	NESS agair	nst 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
7	CCTV	Q3.1_1	0.691	0.324	0.272	0.329	0.358
IOI.	database	Q3.1_2	0.268	0.543	0.373	0.368	0.513
D D	SNS	Q3.1_3	0.337	0.444	0.548	0.361	0.500
REDUCTION	financT	Q3.1_4	0.340	0.419	0.446	0.495	0.467
œ	Geoloc.	Q3.1_5	0.325	0.530	0.490	0.468	0.571
7	CCTV	Q3.2_1	0.672	0.298	0.297	0.374	0.401
DETECTION	database	Q3.2_2	0.294	0.519	0.494	0.337	0.530
ECT	SNS	Q3.2_3	0.337	0.395	0.541	0.315	0.440
DET	financT	Q3.2_4	0.468	0.293	0.356	0.481	0.399
-	Geoloc.	Q3.2_5	0.417	0.367	0.413	0.362	0.534
N	CCTV	Q3.3_1	0.591	0.319	0.345	0.322	0.380
Ĕ	database	Q3.3_2	0.333	0.486	0.384	0.258	0.474
ECL	SNS	Q3.3_3	0.213	0.374	0.401	0.191	0.377
PROSECUTION	financT	Q3.3_4	0.391	0.312	0.297	0.417	0.346
РВ	Geoloc.	Q3.3_5	0.413	0.329	0.329	0.367	0.440

Table A9: Correlations – Security and happiness

Usefulness for

			Feeling of			Happiness about			
			SECURITY	ССТV	SNS	Database	FinancT Geoloc.		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	-0.409	1.000					
	SNS	Q5.3_2	-0.372	0.480	1.000				
PIN PIN	Database	Q5.3_3	-0.398	0.389	0.771	1.000			
Fee IAP	FinancT	Q5.3_4	-0.297	0.517	0.615	0.635	1.000		
-	Geoloc.	Q5.3_5	-0.310	0.604	0.749	0.649	0.697	1.000	
Happiness about NOT Q5.4 KNOWING		Q5.4	-0.410	0.261	0.341	0.407	0.317	0.352	1.000

34

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	0.071	-0.135	-0.062	-0.073	-0.012				
Feeling of control I	Q4.4.1	0.076	-0.155	-0.098	-0.077	-0.071				
Feeling of control II	Q4.4.2	0.091	-0.118	-0.016	-0.101	-0.028				
Trust I	Q4.5.1	0.046	-0.233	-0.133	-0.156	-0.195				
Trust II	Q4.5.2	-0.022	-0.13	-0.068	-0.124	-0.107				

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	0.594	1.000					
Feeling of security	Q4.3	0.367	0.716	1.000				
Feeling of control I	Q4.4.1	0.320	0.482	0.475	1.000			
Feeling of control II	Q4.4.2	0.284	0.472	0.535	0.736	1.000		
Trust I	Q4.5.1	0.261	0.497	0.595	0.622	0.620	1.000	
Trust II	Q4.5.2	0.230	0.488	0.497	0.531	0.718	0.728	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	0.465	0.115	0.229	0.22	0.208			
Feeling of control I	Q4.4.1	0.228	0.194	0.214	0.097	0.171			
Feeling of control II	Q4.4.2	0.217	0.104	0.262	0.146	0.158			
Trust I	Q4.5.1	0.308	0.16	0.184	0.19	0.236			
Trust II	Q4.5.2	0.186	0.094	0.16	0.1	0.146			

			Answer = YES					
		Total	18-24	25-34	35-44	45-54	55-64	65+
Q1_1	Biometric data , e.g. analysis of fingerprints, palm prints, facial or body features	52.5%	68.0%	67.5%	56.8%	58.8%	53.1%	9.4%*
Q1_2	"Suspicious" behaviour , e.g. automated detection of raised voices, facial or body features	31.0%	32.0%	37.5%	54.1%*	29.4%	18.8%	9.4%*
Q1_3	Data and traffic on the internet , e.g. Deep Packet/Content inspection	25.5%	20.0%	35.0%	37.8%	29.4%	21.9%	3.1%*
Q1_4	Databases containing personal information, e.g. searching state pension databases, or customer databases of private companies	41.0%	52.0%	62.5%*	56.8%	38.2%	21.9%	9.4%*
Q1_5	Online communication , e.g. social network analysis, monitoring of chat rooms or forums	52.5%	60.0%	87.5%*	62.2%	52.9%	40.6%	3.1%*
Q1_6	Telecommunication , e.g. monitoring of phone calls or SMS	61.0%	96.0%*	85.0%	59.5%	61.8%	50.0%	15.6%*
Q1_7	Electronic tagging / Radio Frequency Identification (RFID), e.g. tracking geolocation with electronic chips implanted under the skin or in bracelets	31.0%	36.0%	40.0%	40.5%	38.2%	25.0%	3.1%*
Q1_8	Global Positioning Systems (GPS), e.g. tracking geolocation of cars or mobile phones	60.0%	72.0%	82.5%	70.3%	64.7%	53.1%	12.5%*
Q1_9	CCTV cameras , e.g. in public places, airports or supermarkets	65.5%	72.0%	65.0%	70.3%	76.5%	68.8%	40.6%*
Q1_10	Financial information , e.g. tracking of debit/credit card transactions	53.0%	68.0%	67.5%	59.5%	61.8%	34.4%	25.0%*

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?

Note: Results in this table marked with an asterisk (*) show a statistically significant difference (p<.05) from all other age groups; for all other results the respective tests did not show a statistically significant difference between the individual age groups.

Table A14: Known reasons for surveillance by age group

			Answer = YES							
		Total	18-24	25-34	35-44	45-54	55-64	65+		
Q2_1	The reduction of crime	50.0%	60.0%	60.0%	54.1%	55.9%	37.5%	31.3%		
Q2_2	The detection of crime	56.5%	60.0%	75.0%	64.9%	58.8%	59.4%	15.6%*		
Q2_3	The prosecution of crime	52.0%	68.0%	70.0%	51.4%	55.9%	53.1%	12.5%*		
Q2_4	Control of border-crossings	37.0%	44.0%	45.0%	43.2%	50.0%	28.1%	9.4%*		
Q2_5	Control of crowds	34.5%	20.0%	55.0%*	43.2%	29.4%	28.1%	21.9%		
Q2_6	Other	25.5%	16.0%	25.0%	29.7%	26.5%	21.9%	31.3%		
Q2_7	I don't know of any reasons.	7.5%	0.0%	5.0%	2.7%	11.8%	19.5%	5.6%		

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

Note: Results in this table marked with an asterisk (*) show a statistically significant difference (p<.05) from all other age groups); for all other results the respective tests did not show a statistically significant difference between the individual age groups.

Table A15: Feelings of security, control and trust by age group

		Total				18-24	3-24		25-34		35-4	35-44	
4.3	Security (1=very insecure; 5=very secure)	Mea	n STI	D	Mea	an	STD	Me	an	STD	Mean	STD	
	How secure does the presence of surveillance measures make you feel	1.95	5 1.00	08	2.1	6	1.068	3 2.3	81 ^A	0.79	5 2.09	1.201	
4.4	Control (1= no control; 7=full control)												
4.4.1	Control over processing of personal information gathered via government agencies	1.67	7 1.03	33	2.0	4	1.060	0 1.5	56	0.843	3 2.21 ^{AB}	1.386	
4.4.2	Control over processing of personal information gathered via private companies	1.72	2 1.07	73	2.46 ⁴	ABCD	1.141	1 1.5	5 ^{ae}	0.86	0 2.29 ^{EFGH}	1.384	
4.5	Trust (1=no trust; 7=complete trust)												
4.5.1	Trust into government that they protect personal information	1.79	9 1.05	54	2.16	5^	1.143	3 1.7	78	0.80	D 2.11 ^B	1.260	
4.5.2	Trust into private companies that they protect personal information	1.71	0.95	57	2.42 ⁴	BCD	1.018	3 1.7	′4 ^A	0.850) 1.89 ^E	1.157	
			45	-54			55-64	4		65+			
4.3	Security (1=very insecure; 5=v secure)	ery	Mean	S	TD	Mea	an	STD	Me	ean	STD		
	How secure does the presence surveillance measures make yo feel		1.50		.648			1.118			0.805		
4.4	Control (1= no control; 7=full control)												
4.4.1	Control over processing of personal information gathered government agencies	via	1.34 ^A	0.	.814	1.	48 ().849	1.	21 ^в	0.631		
4.4.2	Control over processing of personal information gathered private companies		1.22 ^{bf}	0.	506	1.52	2 ^{cg} ().935	1.1	7 ^{DH}	0.576		
4.5	Trust (1=no trust; 7=complete trust)												
4.5.1	Trust into government that the protect personal information	ey	1.62	1.	.049	1.	71 1	1.117	1.2	2 ^{AB}	0.600		
4.5.2	Trust into private companies the they protect personal informated and the they protect personal informated and the the the term of ter		1.55 ^B	0.	948	1.4	1 ^c (0.636	1.1	.8 ^{de}	0.501		

Q4.3: How secure does the presence of surveillance measures make you feel? (1=very insecure, 5=very secure)

Q4.4.1/Q4.4.2: How much control do you think you have over the processing of your personal information gathered via government agencies/private companies? (1=no control, 5=full control)

Q4.5.1/Q4.52: How much do you trust government agencies/private companies that they protect your personal information gathered via surveillance measures? (1=no trust, 5=complete trust)

Note: Results marked with a letter in superscript, e.g. (^A), indicate that the result is statistically significantly different from the result in the same row (question) marked with the same letter. Other results not marked with a superscript are not statistically significantly different between age groups for that question.

Table A16: Happiness with surveillance by age group

		Total		18-	18-24		25-34		35-44	
	Happy/unhappy with surveillance (1=very happy, 5=very unhappy)	Mean	STD	Mean	STD	Mean	STD	Mean	STD	
5.4	Feel happy/unhappy about surveillance taking place without noticing	4.03	1.010	3.55 [^]	1.260	3.89	0.980	3.97	0.760	
		4	45-54		55-64		65+			
	Happy/unhappy with surveillance (1=very happy, 5=very unhappy)	Mea	n STE) Mea	in STI	D Mea	n STI)		
5.4	Feel happy/unhappy about surveillance taking place without noticing	4.2	4 1.00	00 4.0	00 1.05	50 4.42	2^ 0.96	50		

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

Note: Results marked with a letter in superscript, e.g. (^A), indicate that the result is statistically significantly different from the result in the same row (question) marked with the same letter. Other results not marked with a superscript are not statistically significantly different between age groups for that question.

Table A17: Awareness of CCTV by age group

Q5.2.1	Which of the following best describes you?	Total	18-24	25-34	35-44	45-54	55-64	65+
					10.8			12.5
	I never notice CCTV cameras.	7.5%	4.0%	10.0%	%	0.0%	6.3%	%
		23.0	44.0%	40.0%	13.5	14.7		15.6
	I rarely notice CCTV cameras.	%	*	*	%	%	12.5%	%
		30.0			32.4	38.2		31.3
	I sometimes notice CCTV cameras.	%	28.0%	25.0%	%	%	25.0%	%
		25.0			27.0	32.4		25.0
	I often notice CCTV cameras.	%	20.0%	20.0%	%	%	25.0%	%
		10.5			10.8	11.8	25.0%	
	I always notice CCTV cameras.	%	4.0%	2.5%	%	%	*	9.4%
	I don't know / No answer	4.0%	0.0%	2.5%	5.4%	2.9%	6.2%	6.2%

Q5.2.1: Which of the following best describes you?

Note: Results in this table marked with an asterisk (*) show a statistically significant difference (p<.05) from all other age groups; for all other results the respective tests did not show a statistically significant difference between the individual age groups.

Table A18: Beliefs about economic costs of surveillance by age group

Q6.2	Total	18-24	25-34	35-44	45-54	55-64	65+
far too little	7.0%	8.0%	10.0%	10.8%	5.9%	3.1%	3.1%
too little	12.5%	24.0%	17.5%	13.5%	11.8%	3.1%	6.3%
just right	15.0%	20.0%	17.5%	21.6%	11.8%	12.5%	6.3%
too much	11.0%	8.0%	10.0%	13.5%	14.7%	3.1%	15.6%
far too much	20.5%	4.0%	7.5%	16.2%	20.6%	34.4%	40.6%*
I don't know	33.0%	36.0%	37.5%	24.3%	35.3%	37.5%	28.1%
No answer	1.0%	0.0%	0.0%	0.0%	0.0%	6.3%	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 (*) show a statistically significant difference (p<.05) from all other age groups; for all other results the respective tests did not show a statistically significant difference between the individual age groups.

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	l don't know
Surveillance using databases containing personal information	1 Not at all useful	2	3	4	5 Very useful	l don't know
Surveillance of online social networking	1 Not at all useful	2	3	4	5 Very useful	l don't know
Surveillance of financial transactions	1 Not at all useful	2	3	4	5 Very useful	l 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	l 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	l don't know
Surveillance using databases containing personal information	1 Not at all useful	2	3	4	5 Very useful	l don't know
Surveillance of online social networking	1 Not at all useful	2	3	4	5 Very useful	l don't know
Surveillance of financial transactions	1 Not at all useful	2	3	4	5 Very useful	l 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	l 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	l don't know
Surveillance using databases containing personal information	1 Not at all useful	2	3	4	5 Very useful	l don't know
Surveillance of online social networking	1 Not at all useful	2	3	4	5 Very useful	l don't know
Surveillance of financial transactions	1 Not at all useful	2	3	4	5 Very useful	l 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	l 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 government agencies?

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	Rarely	Sometimes	Often	Happens all	l don't
	happens	happens	happens	happens	the time	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	Нарру	Neither happy nor unhappy	Unhappy	Very unhappy	l 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?

		Geolocation surveillance (Using mobile phones,
	ссту	GPS, electronic tagging,
		or RFID to determine the
		location of the devices
		and the devices' owners)
Public services (e.g. local council offices)	Acceptable	Acceptable
	Unacceptable	Unacceptable
	🗆 I don't know	🗆 I don't know
Private companies (e.g. banks)	Acceptable	Acceptable
	Unacceptable	Unacceptable
	🗆 I don't know	🗆 I don't know
Workplace	Acceptable	Acceptable
	Unacceptable	Unacceptable
	🗆 I don't know	🗆 I don't know
Schools / universities	Acceptable	Acceptable
	Unacceptable	Unacceptable
	🗆 I don't know	🗆 I don't know
Clinics and hospitals	Acceptable	Acceptable
	Unacceptable	Unacceptable
	🗆 I don't know	🗆 I don't know
Airports	Acceptable	Acceptable
	Unacceptable	Unacceptable
	🗆 I don't know	🗆 I don't know
Public transport	Acceptable	Acceptable
(Railway, subway, buses, taxis etc.)	Unacceptable	Unacceptable
	🗆 I don't know	🗆 I don't know
City centres	Acceptable	Acceptable
	Unacceptable	Unacceptable
	🗆 I don't know	🗆 I don't know
Specific areas that experience increased crime	Acceptable	Acceptable
rates	Unacceptable	Unacceptable
	🗆 I don't know	🗆 I don't know
Urban spaces in general	Acceptable	Acceptable
	Unacceptable	Unacceptable
	🗆 I don't know	🗆 I don't know
Mass events (concerts, football games etc.)	Acceptable	□ Acceptable
	Unacceptable	Unacceptable
	🗆 I don't know	🗆 I don't know
The street/neighbourhood where I live	Acceptable	Acceptable
	Unacceptable	Unacceptable
	🗆 I don't know	🗆 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 accept- able in all circum- stances	Acceptable only if the citizen is suspected of wrong- doing	Acceptable if the citizen is suspected of wrong- doing and the surveillance is legally authorised	Acceptable if the citizen is informed	Acceptable if the citizen has given consent	Not acceptable in any circum- stances	l 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 accept- able in all circum- stances	Acceptable only if the citizen is suspected of wrong- doing	Acceptable if the citizen is suspected of wrong- doing and the surveillance is legally authorised	Acceptable if the citizen is informed	Acceptable if the citizen has given consent	Not acceptable in any circum- stances	l 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