RAND EUROPE

Public Perception of Security and Privacy

Results of the comprehensive analysis of PACT's pan-European Survey

Sunil Patil, Bhanu Patruni, Hui Lu, Fay Dunkerley, James Fox,
Dimitris Potoglou, Neil Robinson

For more information on this publication, visit www.rand.org/t/rr704

This study has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285635 [PACT - Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action]. This report, which is a project deliverable (D4.2), is also available on the project website www.projectpact.eu

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

Document Management

PROJECT FULL TITLE	Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research into Action
PROJECT ACRONYM	PACT
	Collaborative Project funded under Theme SEC-2011.6.5-2 'The relationship between human privacy and security'
GRANT AGREEMENT	285635
STARTING DATE	01/02/2012
DURATION	36 months

'Public Perception of Security and Privacy: Results of the comprehensive analysis of PACT's pan-European survey'

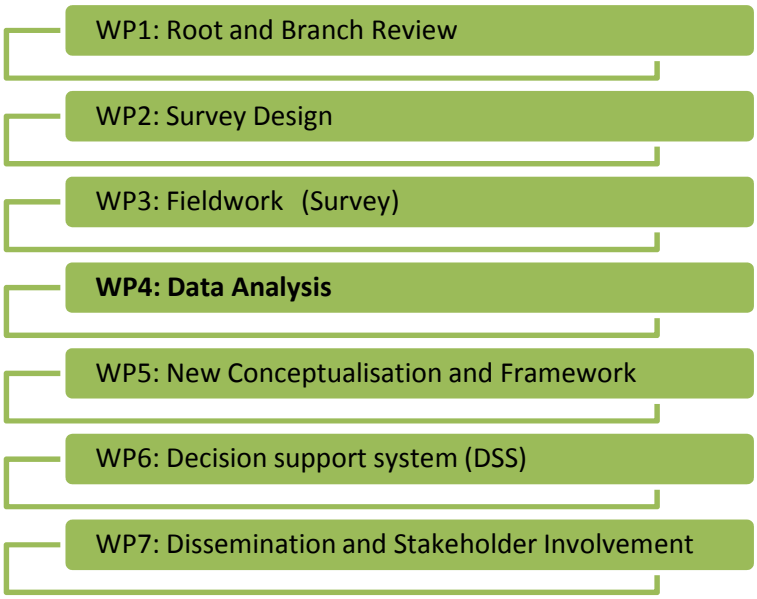
Task: 4.2

Leader: RAND Europe – Other contributors: n/a
Authors: Sunil PATIL, Bhanu PATRUNI, Hui LU, Fay DUNKERLEY, James FOX, Dimitris POTOGLOU, Neil ROBINSON

Executive summary

PACT is a three-year project that aims to understand the public perception of security, privacy and surveillance across the 27 European Union Member States (EU27).[1] The project consortium consists of an expert team with varied backgrounds. The knowledge gained will be used to inform the development of a new Privacy Reference Architecture and Decision Support System, which may help end-users to evaluate the pros and cons of specific security investments on the basis of the societal perception of privacy and liberty.

The PACT project is divided into seven technical work packages, as shown in Figure ES-1. Work Packages 2 to 4 of PACT cover the design, empirical fieldwork and analysis of a pan-European survey of individuals' preferences regarding privacy and security. This deliverable marks the conclusion of Work Package 4 (WP4) – Data Analysis.



ES-1: The seven technical work packages

Work Package 4 focuses on the analysis of stated preferences relating to security, surveillance and privacy

WP4 builds upon PACT's Work Packages 2 and 3.[2,3] WP2 involved the design of a survey instrument to measure public preferences and perceptions relating to security and privacy. WP3 implemented the survey fieldwork across the EU27 using both online and face-to-face surveys.

PACT's empirical questionnaire is based on three stated preference experiments that corresponded to:

1. Choice to travel on metro or train (**Travel**)
2. Choice of an Internet Service Provider (**Internet**)
3. Choice to purchase a device or service for storing health information (**Health**).

[1] At the time of inception of this project (in 2012) there were only 27 Member States of the EU. Croatia joined the EU in 2013 and was not included in the scope of this project.
[2] PACT D2.3 Report on the analysis of pilot data. Available from: http://www.projectpact.eu/deliverables/wp2-survey-design
[3] PACT D3.1 Summary of findings from the survey testing phase. Available from: http://www.projectpact.eu/deliverables/wp3-fieldwork

In WP4, the stated preference data collected in WP3 has been analysed to inform our understanding of the perception of security, privacy, and surveillance across the EU27. WP4 was split into two tasks:

In Task 4.1, some preliminary analysis of the empirical data was performed. The deliverable (D4.1[4]) focused on the methods of data collection, the representativeness of the responses, the quality of stated preference data and respondents' understanding of the choice experiments. The report outlined initial findings relating to attitudes, including those towards trust, privacy and security at the country level. The report also presented a summary of preferences relating to privacy, security and surveillance, analysed using preliminary discrete choice models.

Task 4.2 builds upon the work undertaken in Task 4.1. In Task 4.1, initial choice models were developed for the Travel, Internet and Health models. In Task 4.2 these initial models have been extended to take account of country-specific effects. The models have also been extended to take account of socio-economic factors, which include age, gender, education, work status and income.

Below we set out our key findings.

Preferences in the Travel context are related to security and surveillance measures at train/metro facilities

Regarding preferences for privacy, security and surveillance expressed by participants in the context of travelling by metro/train, we find that respondents are in favour of CCTV cameras (including ones with additional features such as face recognition) that store data for a certain amount of time and which can be accessed by police departments within the country. In general, people of all age groups across the EU27 prefer having CCTV cameras. However, the preference is weaker for young people (aged 18 to 24) and stronger for those aged between 55 and 64. In addition, we observe that, while both males and females prefer having CCTV cameras, females have stronger preference compared to males across the EU27. In the majority of countries, respondents prefer having security personnel at stations, but that the security personnel are unarmed. Interestingly, respondents in France preferred armed police compared to security forces employed by private companies. While, in most countries, participants exhibited aversion to any type of security checks, in some countries, there was a weaker disinclination towards physical searches, with stand-off technologies such as metal detectors preferred over more intrusive (and slower) forms of check such as physical searching. Young people (18 to 24) across the EU27 indicate a stronger disinclination towards physical checks involving metal detectors/full body scanners compared to other age groups. Unsurprisingly, respondents are more likely to choose alternatives that incur little delay due to physical security checks or have no additional cost due to security and surveillance measures. Our analysis suggests that people may exhibit complex preferences between privacy, security and convenience given the preferences for stand-off technologies (which, it may be assumed, are perceived to be much quicker than physical checks).

Preferences in the Internet context are related to surveillance of Internet usage

Aside from three countries, respondents prefer Internet Service Providers (ISPs) that do not collect, store or allow access to their Internet usage data. While people of all age groups across the EU27 are generally averse to any level of storage of information on their Internet usage, younger people (18 to 24) are less averse to storage of information on the websites they have used. Females and respondents with lower

[4] PACT D4.1 Headline Findings. Available from: http://www.projectpact.eu/deliverables/wp4-data-analysis

secondary education are less strongly averse to all levels of information storage. Respondents exhibit preferences for ISPs providing privacy friendly services, such as actively hiding Internet usage data and warning users which websites do not meet their desired level of privacy, with those over the age of 65 having stronger preferences. Respondents' views on Internet surveillance are less consistent across the EU27. On average, most respondents prefer that surveillance can take place 'only with a warrant' and they are averse to having more intrusive levels of surveillance. People over the age of 65 are less averse to higher levels of surveillance than other age groups. Those in the 55 to 64 age group are, however, more concerned about police surveillance without a warrant during a state of emergency. Despite this, respondents are less likely to choose ISPs that never allow continuous surveillance of Internet users over ISPs that allow surveillance with a warrant. The preference for accountable surveillance and for ISPs that do not store personal information is suggestive of a rather more nuanced understanding of privacy concerns than a simple good-bad binary trade-off model would suggest. Finally, respondents are willing to pay for such services, a finding which illuminates the possibility that there is a market for Privacy Enhancing Technologies (PETS). This, coupled with our analysis of the extent of preferences in other areas, suggests that individuals have an appetite for privacy enhancing measures and that they are willing to pay for them. It is unclear the extent to which the recent public debate about the surveillance capabilities of intelligence agencies has influenced these preferences.

Preferences in the Health context are related to storage of health records

We find that in the Health context a less conservative picture emerges, with respondents from most countries and all age groups preferring a device/service that allows storage of personal identification data and data on lifelong health conditions in addition to basic health data. Moreover, younger people (18–34) express a preference for a device storing their full medical history. The additional access to information by paramedics is preferred over limiting access to only doctors and nurses. However, additional access to fire and rescue personnel is not preferred. We also see that respondents are averse to insurance providers, pharmaceutical companies or researchers having access to their health information. Regarding potential costs, respondents are willing to pay a premium for such a device if it represents some of the alternatives discussed above (e.g. storage of personal identification data and data on lifelong health conditions, access to paramedics as well as doctors and nurses).

Attitudes influence preferences relating to security, surveillance and privacy

Structural Equation Modelling (SEM) was used to represent the relationships between socio-economic variables and the responses to the attitudinal questions. In the models developed for all three contexts, attitudes are found to be influenced by age, gender and income. Furthermore, education level is found to influence attitudes in the Internet and Health contexts, but no significant effect was identified for attitudes in the Travel context. Context-specific factors, such as travel frequency, time spent on the Internet, and current health condition, were additionally found to play a role.

Respondents' attitudes significantly affect their preferences in relation to privacy, security and surveillance. The more distrustful (to business, voting, government and technology) a respondent is, the greater their concern for privacy, and it is more likely that the respondent will choose the 'none of these' alternative across all experiments.

The link between attitudes and individuals' preferences in the experiments is also intuitive. For example, with regard to the collection of information when using the Internet, respondents whose attitudes indicate a high level of concern for privacy are more likely to choose alternatives that involve less storage of data. At

the same time, they are in favour of some level of Internet surveillance, which suggests that respondents may perceive surveillance to be privacy enhancing to a certain degree.

Clear differences in preferences for privacy, security and surveillance are found, depending on the context

The results for Travel, Internet and Health highlight how dependent preferences for privacy, security and surveillance are on context. Most respondents across the EU are found to prefer some level of data storage on CCTV cameras or on a health device; the preference for CCTV cameras also indicates a preference for surveillance. However, they dislike any storage of information on Internet usage or monitoring of their Internet activities by the police, except when there is a genuine need (a warrant having been issued by a judge/court). Indeed they prefer that their ISP offers some services to improve online privacy.

Preferences for security and privacy are surprisingly consistent across the EU

Despite the different preferences between contexts, the results are quite consistent across the 27 EU Member States surveyed, although there are some country-specific effects. These particularly concern the presence of security personnel and security checks in the Travel context and viewing of data by different groups other than medical practitioners in the Health setting.

Socio-economic effects were also found to play a role. In terms of surveillance, older people (65+) are generally less averse to the presence of CCTV cameras or Internet surveillance and had stronger preferences for services to improve online privacy. Younger people (18–24), on the other hand, are more open to storage of their Internet and health data, but are more averse to physical security checks.

Overall, the results indicate that respondents' preferences relating to security and privacy are much more nuanced than the simplistic inverse relationship between security and privacy that is often assumed; this is an important finding from a policymaking perspective.

Table of contents

Table of figures

Table of tables

List of abbreviations

Abbreviation	Meaning
CCTV	Closed Circuit Television
EU27	Member States of the European Union (excluding Croatia)
GCHQ	Government Communications Head Quarters
ICLV	Integrated Choice and Latent Variable
ISP	Internet Service Provider
NSA	National Security Agency
PACT	Public perception of privacy and security: Assessing knowledge, Collecting evidence and Translating research into action
SEM	Structural Equation Model
SP	Stated Preference
WP	Work Package
WTA	Willingness to Accept
WTP	Willingness to Pay
Country codes	
BE	Belgium
BG	Bulgaria
CZ	Czech Republic
DK	Denmark
DE	Germany
EE	Estonia
IE	Ireland
EL	Greece
ES	Spain
FR	France
IT	Italy
CY	Cyprus
LV	Latvia
LT	Lithuania
LU	Luxembourg
HU	Hungary
MT	Malta
NL	Netherlands
AT	Austria
PL	Poland
PT	Portugal
RO	Romania
SI	Slovenia
SK	Slovakia
FI	Finland
SE	Sweden
UK	United Kingdom

1. Introduction

PACT (Public perception of privacy and security: Assessing knowledge, Collecting evidence and Translating research into action) is a three-year project aimed at understanding the public perception of security and privacy across 27 European Union Member States (EU27). The project consortium consists of experts from a variety of backgrounds. As presented in Figure 1, the PACT project is divided into seven technical work packages (WPs) designed to achieve the following objectives:

1. To assess existing knowledge about public perception of privacy and security (WP1).
2. To collect empirical evidence about the way in which European citizens perceive and assess the relationship between privacy and security (WP2–WP4).
3. To develop and validate a prototype Decision Support System, which may help end-users to evaluate the pros and cons of specific security investments on the basis of the societal perception of privacy and liberty (WP5–WP7).

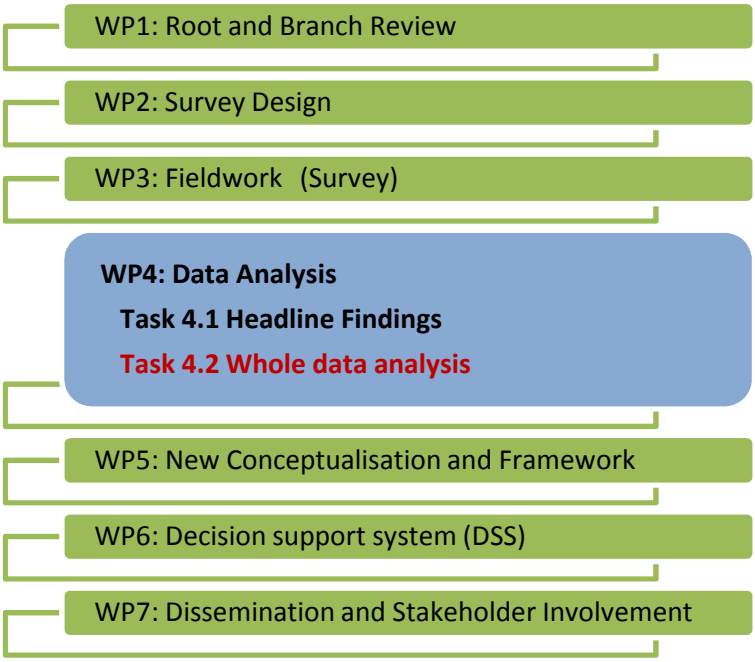


Figure 1: The seven technical work packages

RAND Europe is leading the empirical work in WP2 and WP4. This has been based on the Stated Preference (SP) methodology, which involves collecting respondents' preferences using scenarios based on real-life situations. RAND Europe has worked closely with other consortium partners in order to benefit from and inform the work undertaken in these work packages. This report marks the conclusion of WP4 and provides a summary of the detailed analysis undertaken in Task 4.2. A brief summary of WP2 and WP3 is provided below.

WP2 focused on the design of the empirical research (Tasks 2.1 to 2.4). To enable collection of the empirical evidence, a survey questionnaire was designed to be deployed in the EU27. The questionnaire contained stated preference choice exercises in three contexts: travel on metro or train; choice of an Internet service provider; and choice to purchase a device or service for storing health-related information. These contexts will hereafter be referred to as Travel, Internet and Health, respectively. The development of the questionnaire was based on a range of hypotheses covering individuals' preferences relating to

security, surveillance and privacy. The hypotheses also cover broader societal and socio-economic issues that can affect these preferences. These hypotheses are listed in PACT D2.4.[5] The development of PACT's questionnaire was also informed by the Knowledge Consolidation Workshop,[6] stakeholder consultation, expert interviews and focus groups.

WP3 focused on data collection (Tasks 3.1 to 3.3). The survey questionnaire developed in WP2 was extensively tested through cognitive interviews and pilot surveys. The pilots were conducted in Denmark, Italy and Romania in May 2013. Using the feedback from the pilot surveys and cognitive interviews the questionnaire was simplified and modified significantly. An additional small pilot was thus undertaken in Romania in July 2013 before starting the main stage of data collection. A sampling strategy[7,8] for the main stage of data collection in each of the EU27 countries was established and the fieldwork was carried out from August to November 2013. Respondents were selected (according to quotas for age, gender and region) to participate either in an online or face-to-face interview. Each respondent participated in up to two stated choice exercises from the three potential contexts: Travel, Internet and Health. It should be noted that the time period for the main stage fieldwork overlapped with publication of news stories covering National Security Agency (NSA) and Government Communications Head Quarters (GCHQ) secret surveillance, which might conceivably have influenced some responses due to heightened awareness of issues relating to privacy. However, it is not possible to isolate the effect of this development, which would have required collection of longitudinal data (ideally from the same respondents) before and after the event.

The main objective of WP4 is to provide empirical evidence on the relationship between privacy and security through analysis of the data collected in WP3. While analysis of preferences relating to security and privacy is the focus of the empirical work, the data analysis also considers attitudes, perceptions and contextual information relating to security and privacy.

The empirical work for WP4 is divided into two tasks and the results of the first of these, Task 4.1 (Headline Findings), are reported in D4.1.[9] In this task, an initial review of the data was carried out to identify factors that would require careful consideration in the analysis of stated preferences. In particular, the review investigated: the national representativeness of data; the relevance of the three contexts chosen to implement the stated preference exercises; respondents' understanding of and engagement with the stated preference exercises; and attitudes and perceptions relating to trust, privacy and security. Having established the robustness of the sampled data, preliminary analyses of stated preferences relating to security and privacy were undertaken using discrete choice models.[10] The observations relating to the descriptive analysis of data were also discussed in a workshop[11] involving RAND Europe (responsible for WP4) and Ipsos (responsible for data collection in WP3).

Task 4.2 (Whole Data Analysis) builds on the preliminary analysis of Task 4.1. It focuses on the development of detailed discrete choice models, refining the basic models estimated in Task 4.1 to provide a better understanding of security and privacy preferences. Specifically, the task involves identifying sub-groups of

[5] PACT D2.4 A Note on PACT's Survey Hypotheses. Available from: http://www.projectpact.eu/deliverables/wp2-survey-design
[6] PACT D2.1 Knowledge Consolidation Meeting Report. Available from: http://www.projectpact.eu/deliverables/wp2-survey-design
[7] PACT D3.1 Summary of findings from the survey testing phase. Available from: http://www.projectpact.eu/deliverables/wp3-fieldwork
[8] PACT D3.2 Sampling report. Available from: http://www.projectpact.eu/deliverables/wp3-fieldwork
[9] PACT D4.1 Headline Findings. Available from: http://www.projectpact.eu/deliverables/wp4-data-analysis
[10] Train, Kenneth, *Discrete Choice Methods with Simulation*, Cambridge University Press, Cambridge, 2009.
[11] PACT D4.1 Headline Findings, Appendix A: Notes from the Task 4.1 workshop.

respondents who may have significantly different preferences compared to others; these could be identified by socio-economic factors such as age, gender and education, or by effects specific to a given country. Task 4.2 also further investigates the effects of attitudes towards privacy, security and trust on respondents' preferences. Finally, the hypotheses that set the scope of WP4 are accepted or refuted based on the findings from the detailed discrete choice models. The analysis conducted in WP4 also informs the subsequent work packages, specifically the design of the Privacy Reference Framework, part of WP5.

This report is organised as follows:

- **Chapter 2** presents the results from the extended discrete choice models. These models are used to analyse the stated preferences of respondents, including country-specific and socio-economic effects, and provide empirical evidence on preferences relating to security and privacy across the EU27.
- **Chapter 3** provides a quantitative analysis of respondents' attitudes to a wide range of factors relating to trust, security and privacy and combines these results with the discrete choice modelling approach. It also provides a summary of analyses conducted to investigate the determinants of attitudes.
- **Chapter 4** summarises the main findings of Task 4.2 in relation to the specific research hypotheses investigated. The chapter also presents policy recommendations.

2. Preferences relating to security, surveillance and privacy

In the survey questionnaire, each respondent participated in up to two stated preference (SP) choice exercises from the three potential contexts: Travel, Internet and Health. Each exercise consisted of examination of five hypothetical scenarios, with each scenario containing three alternatives. Two of these alternatives were described by specific attributes whereas the third reflected a choice response of 'none of these'. The 'none of these' alternative allowed respondents to indicate that they do not prefer the configurations described by the other two alternatives. The five scenarios presented to each individual were selected from a total of 120 different possible scenarios, derived from an underlying experimental design to estimate the main effects of each attribute on respondents' choices. More details on the experimental design are presented in PACT D2.3 (Chapter 8).[12] An example scenario from each context is presented in Figure 2 to 4. It is emphasised that respondents saw five such scenarios within each context, where the attribute values for each scenario were different.

Different attributes, specific to each of the three contexts (Travel, Internet and Health) were used to describe the alternatives in the choice scenarios, and these are described in the sub-sections of this chapter. However, in all cases, choices between the two alternatives (A and B) allowed the respondents to evaluate different configurations of security, surveillance, data handling and privacy. Examination of these choices provides an estimation of the amount they were willing to pay for service improvements or the amount they were willing to accept for service deteriorations.

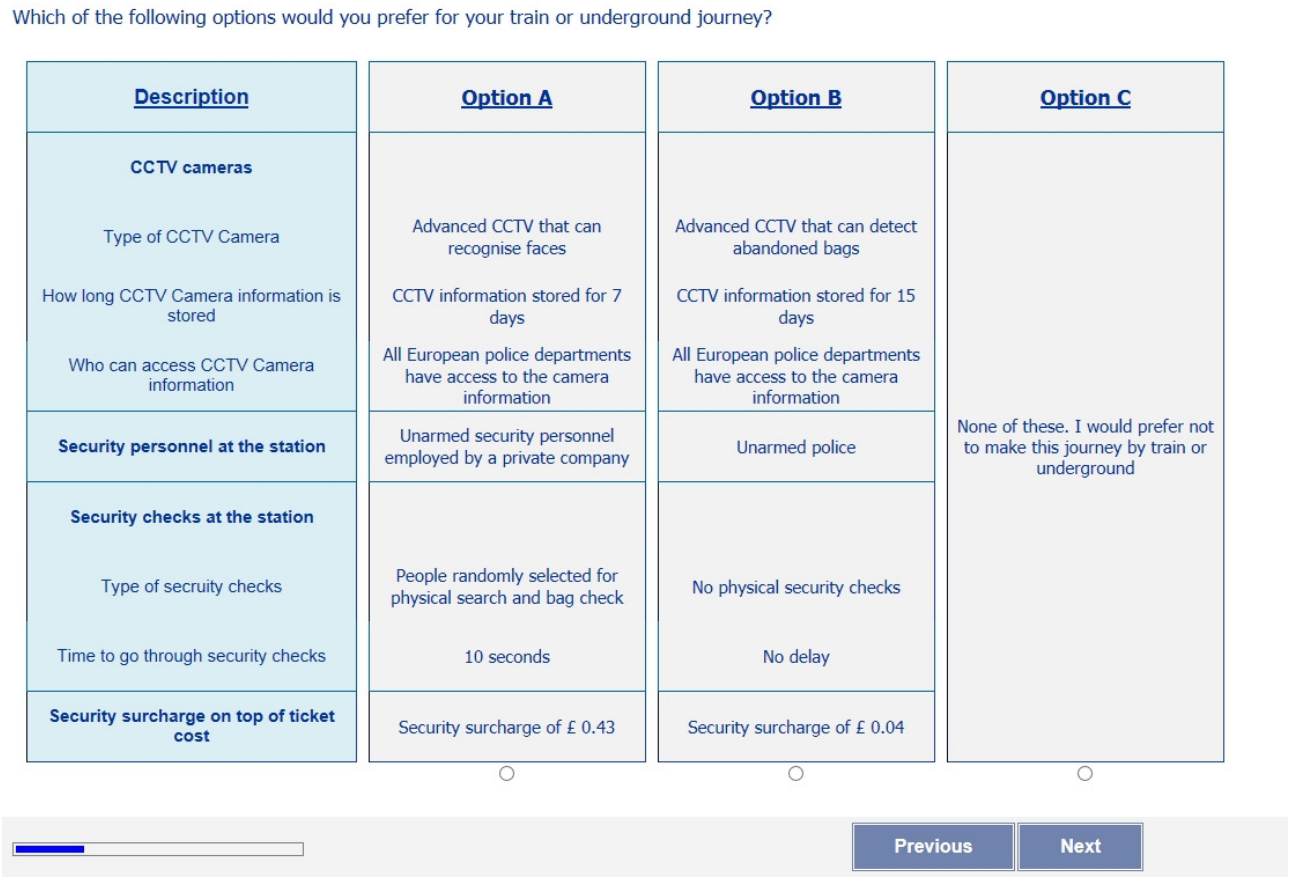


Figure 2: A typical choice scenario in the Travel context

[12] PACT D2.3 Report on the analysis of pilot data. Available from: http://www.projectpact.eu/deliverables/wp2-survey-design

Which of the following options would you prefer as your Internet service provider?

Description	Option A	Option B	Option C
Handling of your internet usage information			
Which internet usage information is stored	Websites you have visited	Websites visited and your location	
How long the information is stored	1 year	6 months	
Who has the access to your information	Information could be shared with all European police departments	Information could only be shared with the police departments in the United Kingdom	None of these, I would prefer to look for another Internet Service Provider
When ISP can allow continuous surveillance of users by the police	Any time without a warrant	Only with a warrant	
Services offered to improve online privacy	ISP will warn you which websites do not meet your desired level of privacy	ISP will advise on how to use Internet anonymously without allowing websites to collect your personal data	
Cost or discount for internet security and data management per month	You **pay** a £ 0.86 premium	You **receive** a £ 0.86 discount	

Previous Next

Figure 3: A typical choice scenario in the Internet context

Which of the following options would you prefer for a health record storage device/system?

Description	Option A	Option B	Option C
What information is stored on the device/system	**Information on device/service**	**Information on device/service**	
Basic health status: blood group, allergies, diabetic status	Basic health status information	Basic health status information	
Identification: name, address, age, photograph, nationality	Identification	Identification	
Lifelong health conditions: asthma, disabilities, cancer, etc.	Lifelong health conditions	Lifelong health conditions	
All health conditions: mental health, sexual health, addictions, and medical history		All other health conditions and medical history	I would not purchase any such device/service
Who can access the information	Doctors, nurses, and emergency medical personnel (paramedics)	Only doctors and nurses	
In which countries your information can be accessed?	Worldwide	Across Europe (EU)	
Who else can view this information apart from the medical specialists?	Health insurance companies	Private sector pharmaceutical companies	
Cost	£ 0.58 per month	£ 2.32 per month	

Previous Next

Figure 4: A typical choice scenario in the Health context

The choices respondents make in the SP experiments provide information on the relative importance of different attributes that describe the alternatives. This information can be objectively evaluated within a random utility theory framework by developing discrete choice models to estimate the weights for each of the attributes and their levels that best reflect the (stated) choices that have been observed. Because each choice scenario also includes a cost element, from the estimation of the choice models we can also derive respondents' willingness to pay using the ratio of attribute weights to the weight on cost.

Discrete choice models[13,14] have been developed for each of the three contexts using the data from all the respondents in the EU27 countries, as described in D4.1. Hence, in these basic models, a single weight is estimated for each of the attribute levels, which could be interpreted as an EU average value. However, even in this case, when pooling data from different country samples it is necessary to consider the possible variation in the unobserved factors or error-variation in the models between countries. These can include different measurement errors across samples and other unobserved cultural and contextual factors. Furthermore, surveys in some countries were carried out online, while others were undertaken 'face to face'. These two types of survey methodology may also give rise to variations in unobserved factors or error-variation in the models, which need to be controlled for. Accordingly, in the development of the discrete choice models, the variation in quality of responses across the following two dimensions is taken into account:

- Country scales[15] to control for country-specific unobserved factors such as difference in quality of data and survey implementation across the EU27.
- Scales by survey methodology[16] to control for variation in response quality between the online and face-to-face survey methodologies. These scale parameters can be identified in addition to the country scales because both survey methodologies were used in Germany and Italy.

The basic models developed for Task 4.1 are further extended in Task 4.2 to include country-specific and socio-economic effects. These effects are considered both for attribute level weights (coefficients) and when a respondent chooses the alternative 'none of these'. Differences in preferences across countries are thus captured by testing whether each country requires a separate attribute level coefficient and/or a separate coefficient for 'none of these'; these are the country specific effects. Using a similar approach, the effects of socio-economic variables such as age, gender, income, education level and working status on the preferences relating to security and surveillance are also included in the discrete choice models. In both cases, only the statistically significant effects at a 95 per cent level of confidence are retained in the final model specification. These results are reported in the following sections.

The choice models developed in Task 4.2 did not take account of the fact that respondents provided more than one observation (each respondent giving five SP choice responses). Accounting for multiple responses using a panel model specification would have increased the time taken for analysis and would not have provided the results to the following work packages in time. Naive models which ignore that individuals provide a number of potentially correlated responses will underestimate the standard errors of the coefficient estimates, leading to inflated levels of statistical significance. Therefore, as a final step in the

[13] Louviere, Jordan J., David A. Hensher and Joffre D. Swait, *Stated Choice Methods: Analysis and Application*, Cambridge University Press, Cambridge, 2000.
[14] Train, Kenneth, *Discrete Choice Methods with Simulation*, Cambridge University Press, Cambridge, 2009.
[15] Bradley, Mark, and Andrew Daly, "New Analysis Issues in Stated Preference Research", in J. de D. Ortúzar (ed.), *Stated Preference Modelling Techniques: PTRC Perspectives 4*, PTRC Education and Research Services Ltd, London, 2000.
[16] Bradley, Mark, and Andrew Daly, "New Analysis Issues in Stated Preference Research", in J. de D. Ortúzar (ed.), *Stated Preference Modelling Techniques: PTRC Perspectives 4*, PTRC Education and Research Services Ltd, London, 2000.

estimation procedure, a 'bootstrap' resampling procedure[17] was applied to correct for model mis-specification and to take account of the repeated nature of the SP data. The application of the 'bootstrap' procedure ensures that the standard errors and t-ratios produced by the models are a realistic statement of the true errors of the model parameters. The detailed results from the choice models include overall model fit statistics, estimated coefficients (including country-level scales and survey methodology scales) and the post-bootstrap t-ratios for each attribute level. These are presented in Appendix A.

All the models are based on a large number of observations across the EU27. Specifically, they are based on 60,472 observations for the Travel context, 74,306 observations for the Internet context, and 94,606 observations for the Health context. Each observation represents a preference indicated in a choice scenario, with each respondent contributing five such observations in each context. The outcome of the stated choice analysis therefore provides robust information on the preferences of respondents in the EU for security and privacy in the three contexts, which can be used to inform policy.

2.1 Choice to travel on metro/train (Travel)

In the Travel survey, respondents were asked to consider scenarios relating to the presence of CCTV cameras, security checks, and type of security personnel at stations. The results are shown in Table A.1 in Appendix A.

2.1.1 Preferences across EU27 countries

In general, we observe similar preferences across countries. Where the preferences differ significantly in a given country these are specifically identified and the effects are presented in the charts below. The values shown in these charts are in the units of utility and can be used for comparison of relative preference between the groups (see Appendix A for description of utility). Furthermore, the charts are presented in a consistent way throughout Chapter 2 and can be interpreted as follows: bars to the right of the vertical axis represent positive preferences, while bars to the left represent a disinclination; the length of a bar is indicative of the strength of a preference relative to the baseline; in each case, 'all other' refers to the EU27 countries, not including the countries identified in the chart as exhibiting different preferences, and is therefore, in most cases, representative of respondents in most EU countries.

Type of CCTV camera

In most EU27 countries, respondents prefer the presence of CCTV cameras compared to the reference level 'No CCTV'. As can be seen from Figure 5, respondents' preferences for the types of CCTV presented are in the following order: advanced CCTVs that can detect faces are most preferred, followed by CCTV that can detect abandoned bags, CCTV that can recognise suspicious movements of people, and standard CCTV (which works like television).

However, the strength of preferences for the different CCTV camera types differs in eleven countries. While all types of CCTV cameras are still preferred over having no cameras in these countries, the magnitude of preference changes for each of them. We observe stronger preference for all types of cameras in France, and stronger preference for standard CCTV cameras over other camera types in Sweden, whereas in Bulgaria, the Czech Republic, Denmark, Greece, Hungary, Latvia, Poland, Portugal and Slovakia the preference for CCTV cameras is weaker compared to other countries in the EU27.

[17] Efron, Bradley, and Robert J. Tibshirani, *An introduction to the bootstrap*, CRC Press, Boca Raton FL, 1994.

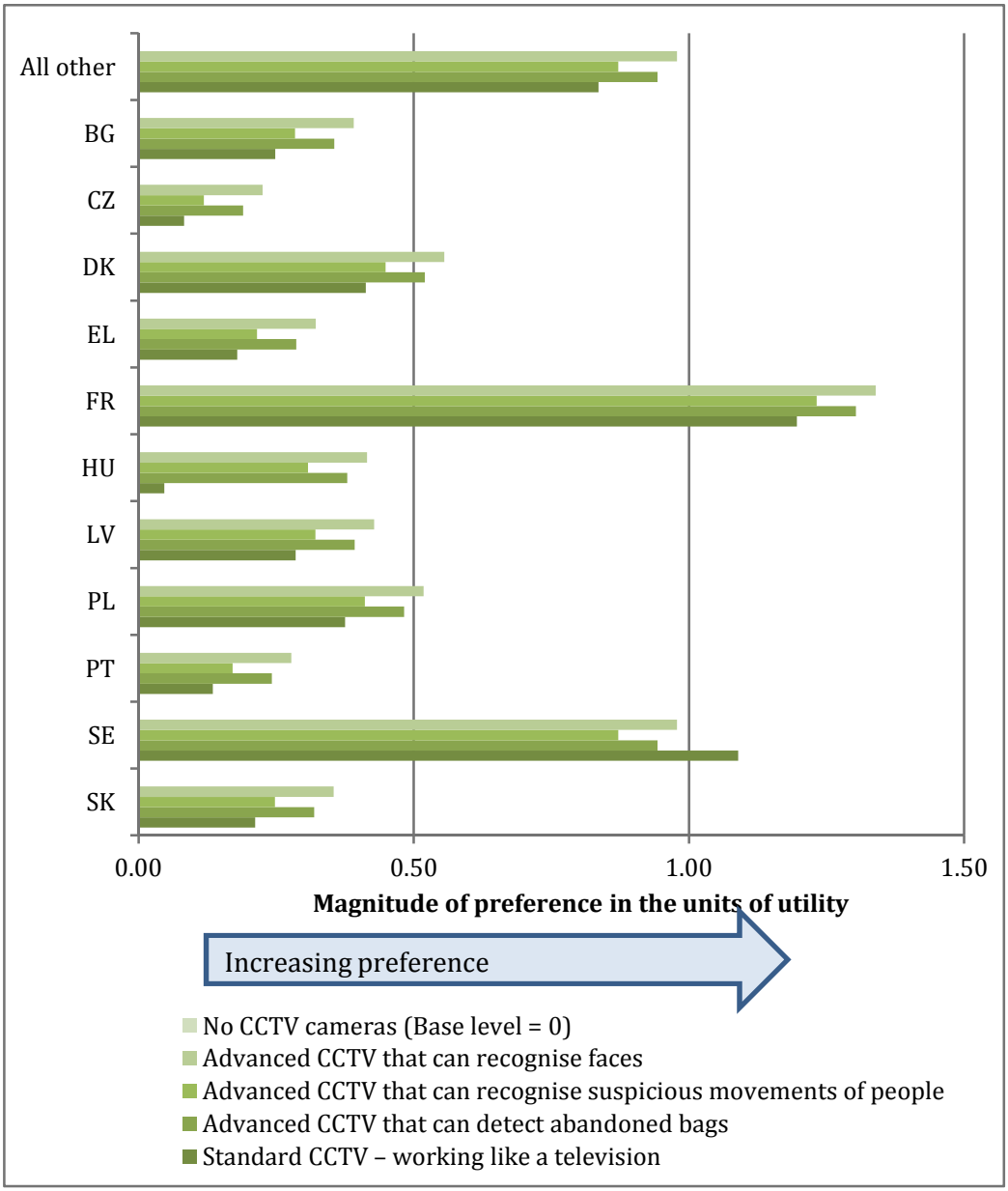


Figure 5: Relative preferences for type of CCTV cameras across the EU27

Duration of storage

In most EU27 countries, given that CCTV cameras are used, respondents prefer that CCTV information is stored for future use, relative to the reference level that CCTV information is only used for real-time monitoring. The magnitude of the coefficients for the duration of storage indicates the respondents' order of preference for storing CCTV information. We observe a U-shaped pattern: 15 days' storage time is the most preferred, followed by 7 days and 3 days; 45 days is the least preferred (see Figure 6).

Contrary to the above preferences in most EU27 countries, respondents in Greece indicate a strong disinclination for storage of CCTV data, preferring real-time monitoring. Furthermore, respondents in the Czech Republic show a disinclination towards storage of CCTV data for 45 days and those in Spain prefer storage for longer durations over shorter ones. Respondents in Estonia and Ireland indicate stronger preferences for data storage over real-time use compared to other countries in the EU27. Respondents in Austria prefer real-time use and medium-term storage (7 to 15 days).

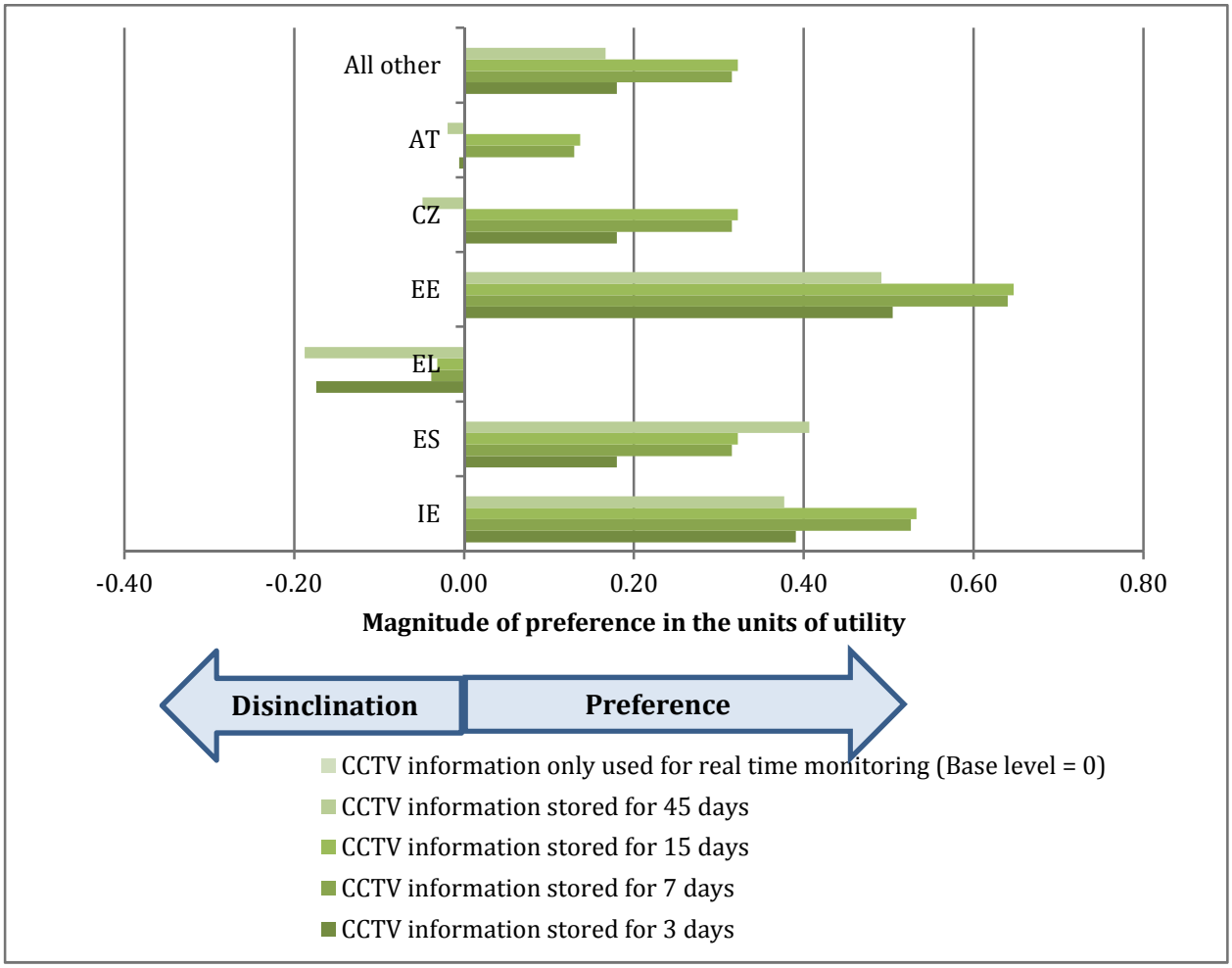


Figure 6: Relative preferences for duration of storage of CCTV data

Access

Across the EU27 respondents show a disinclination towards the option of CCTV information being accessed by police departments outside their home country (across Europe and worldwide), although they are more averse to CCTV information being shared among all police departments worldwide than across only European police departments. Respondents in Germany and Latvia indicate a stronger disinclination towards the option of providing access to all police departments worldwide compared to other countries in the EU27. Additionally, respondents in Latvia are more averse to CCTV information being shared across Europe than other countries in the EU27. These effects are shown in Figure 7.

Security Personnel

In most EU27 countries, respondents prefer having security personnel at train/metro stations relative to the reference level of 'No security personnel' (see Figure 8). Unarmed police are the most preferred option, followed by unarmed security personnel employed by a private company and armed police; armed security personnel employed by a private company are least preferred.

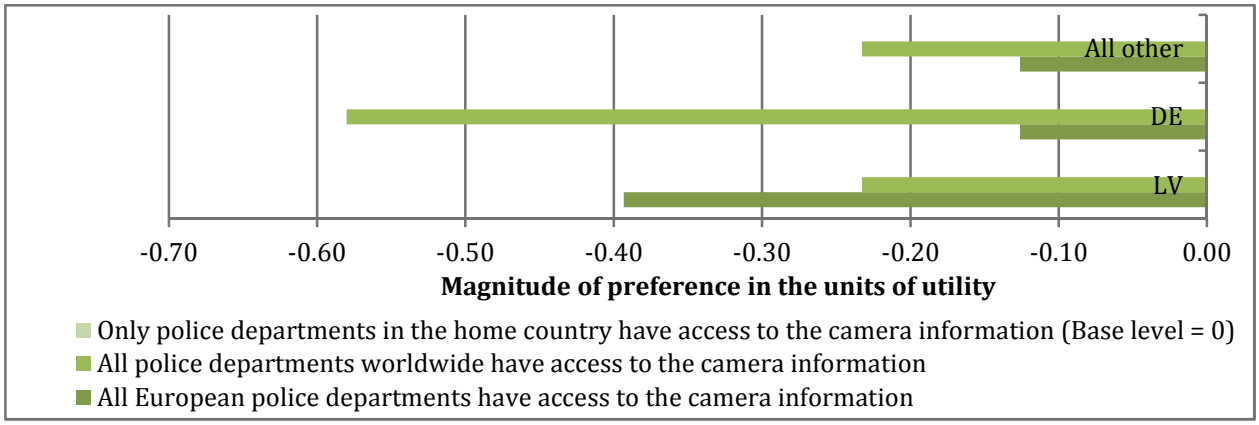


Figure 7: Relative preferences for geographic level of access to CCTV data

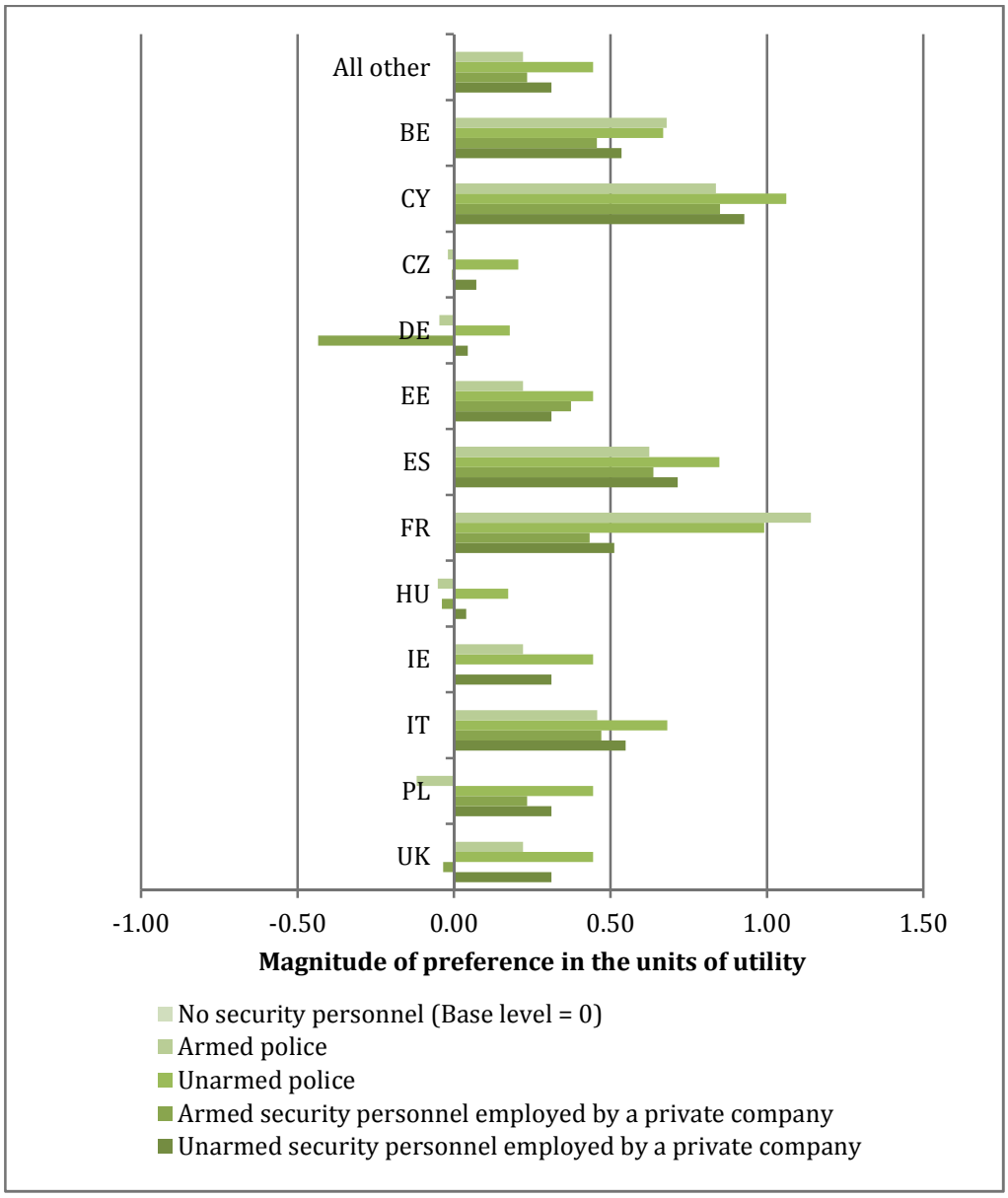


Figure 8: Relative preferences for security personnel

Preferences for security personnel are stronger in Belgium, Cyprus, France, Spain and Italy compared to other countries in the EU27, whereas they are weaker in the Czech Republic, Germany and Hungary.

Contrary to the pattern in other countries, respondents in Germany, Hungary and the UK indicate a disinclination towards armed security personnel employed by a private company compared to no security personnel. Respondents in Germany and Hungary also indicate disinclination towards armed police, along with those in Czech Republic and Poland. Armed security personnel employed by a private company are also less preferred than other security personnel in France and Ireland (however they are still preferred over having no security personnel), whereas in Estonia they are preferred over unarmed personnel employed by a private company. In Belgium and France, armed police are the most preferred type of security personnel, with respondents in France indicating stronger preference for police (armed/unarmed) over private security personnel.

Security Checks

In general, as shown in Figure 9, respondents are averse to having to go through physical security checks, and are more averse to physical searches that include a bag search than going through a full body scanner or metal detector. However, the disinclination towards a physical check involving a metal detector/full body scanner compared to no physical checks becomes statistically insignificant after controlling for country and socio-economic variables. Respondents in more than half the EU27 countries exhibit significantly different preferences for security checks. In Austria, the Czech Republic, Germany, Denmark, Latvia, Poland, Sweden, Slovenia and Slovakia the disinclination is stronger and significant for both types of physical checks. However, respondents in Spain, France and the UK indicate a weaker disinclination towards physical searches that include a bag search and indicate a preference for having a physical check involving a metal detector/full body scanner over no physical security check. Respondents in Italy prefer both types of physical security checks over no physical security checks, whereas those in Bulgaria prefer a physical check involving a metal detector/full body scanner. Respondents in Luxembourg exhibit a stronger disinclination towards metal detectors/full body scanners compared to physical searches and bag checks.

Time to go through security checks

As expected, respondents prefer travel options that take less time to avoid any additional delay due to security checks. No country-specific or socio-economic effects were identified in this attribute.

Security surcharge on top of the ticket (*cost*)

Respondents also dislike paying additional security surcharge, and as expected we see that households with higher incomes are less sensitive to increases in costs (decreasing cost sensitivity with increasing income). In the models, we have merged the 17 income bands into four aggregate bands (monthly income of less than €500, €500 to 1,250, €1,250 to 5,000, and greater than €5,000) – grouping the adjacent bands when the coefficients are not statistically different for individual income bands. A significant proportion (13.7 per cent) of respondents did not provide their income, as they answered ‘prefer not to say’ or ‘don’t know’. A separate coefficient for surcharge on top of the ticket cost is estimated for this group of respondents. Furthermore, the respondents in this group are split by their country of residence using low-, medium- and high-income country groups to account for the wide range of average income across the EU27. Thus the final Travel model contains cost coefficients for seven different groups based on their answers to the income question.

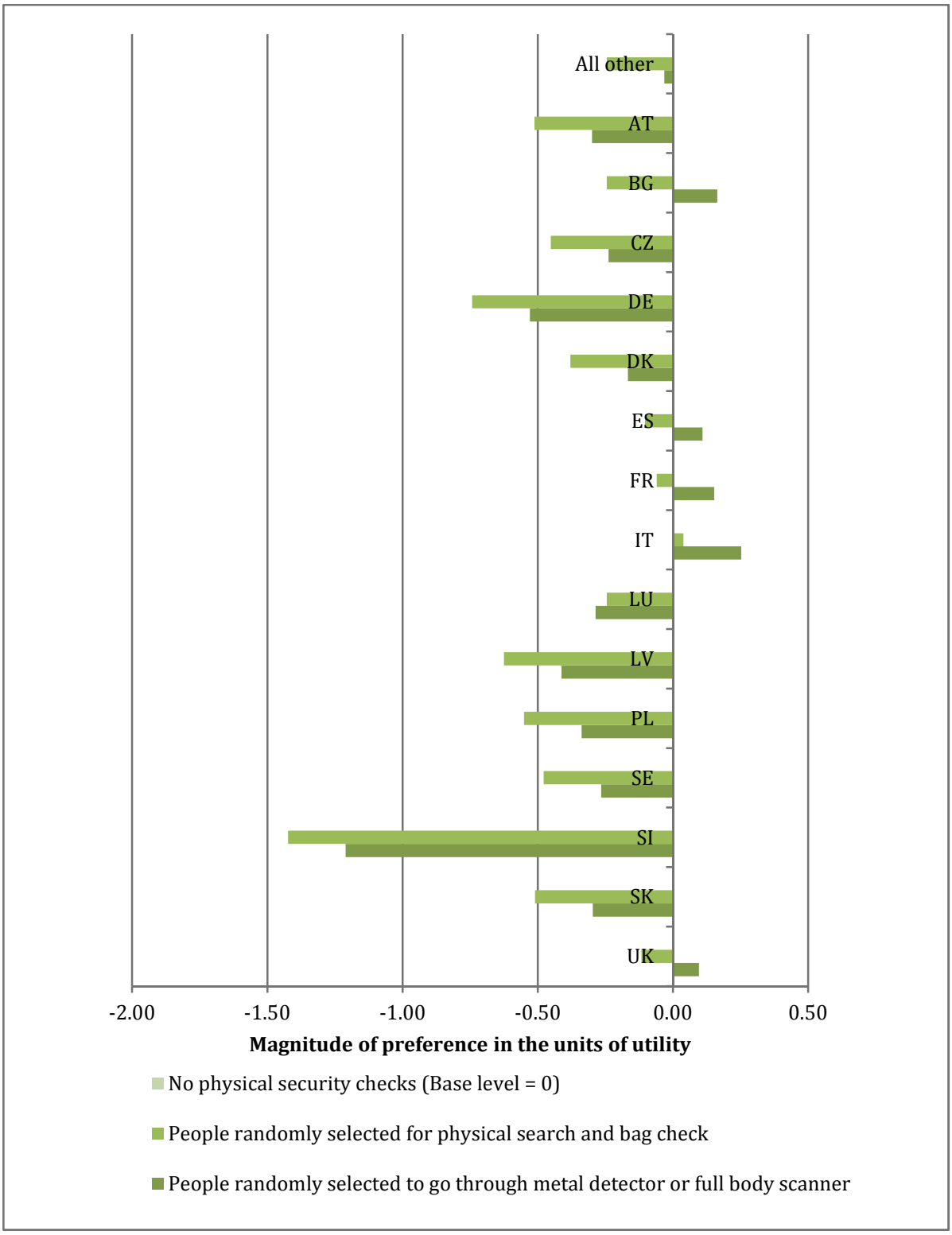


Figure 9: Relative preferences for physical security checks

2.1.2 Differences by socio-economic status

After testing country-specific effects we also tested effects for various socio-economic characteristics, specifically those relating to age (18 to 24, 25 to 34, 35 to 44, 45 to 54, 55 to 64 and 65 plus), gender, working status (full time, part time, looking after family, unemployed, student, retired, not in work due to disability, seeking work, and other), education level, income, and location of residence (big city, suburb, town, village, countryside/farm). These effects are tested on all attribute levels (except on attributes delay and cost) and on the constant for the 'none of these' alternative. We observe the following significant effects:

- In general people of all age groups across the EU27 prefer having CCTV cameras. However, the preference is weaker for young people (aged 18 to 24) and stronger for those aged 55 to 64. In addition, we observe that while both males and females prefer having CCTV cameras, females have stronger preference for CCTV cameras compared to males across the EU27.
- Young people (aged 18 to 24) across the EU27 have a stronger disinclination towards physical checks involving metal detectors/full body scanners compared to other age groups. Also, young people (aged 18 to 24) show a stronger disinclination towards choosing the 'none of these' alternative – indicating that they are more likely to choose alternatives A and B, which present a combination of security, surveillance and privacy levels.

2.1.3 Willingness to pay

Use of the stated preference method in this study allows us to estimate respondents' willingness to pay (WTP) for security or surveillance measures for travel facilities. The willingness to pay valuations are presented in Figure 10 along with their 95 per cent confidence intervals. The zero valuations correspond to the base level in each attribute. The WTP estimates are representative values that apply to the majority of the countries and age groups.[18] In a linear model such as the one used in this study, the WTP is calculated as the negative ratio of the coefficient of a given attribute level to the coefficient of cost.[19] Since all the coefficients in this study (with the exception of delay/time to go through security checks) are estimated with respect to a base level, the WTP value reflects willingness to pay for the level of a given attribute with respect to the base level. As the cost attribute was presented as the per trip ticket cost, the WTP estimates also correspond to the value per trip. Furthermore, the cost coefficient is segregated by income groups allowing the estimation of WTP for each of those groups. As some of the attributes have country-specific effects we report the coefficients and WTP representing the largest group of countries in EU27. We emphasise the caveat that the WTP valuations are derived from stated choice responses, which can provide over- or underestimates of WTP valuations (because people do not actually have to pay for the choices that they make) relative to valuations from real-world behaviour/choices.[20] Nevertheless, the values estimated here are useful for comparison across different attribute levels and are possibly the only EU-wide estimates available in these contexts.

For the respondents from the lowest income group (monthly household income after taxes less than €500), the WTP for CCTV facilities, per trip, is estimated from €1.12 to €1.31 depending on the type of CCTV camera. Respondents are willing to pay up to an additional €0.43 to ensure that data are stored (as

[18] As discussed in the sections above, a number of country-specific and socio-economic effects are identified in the Travel model. Therefore, to get the WTP for each country and age-group these effects need to be taken into account.
[19] Hensher, David A., John M. Rose and William H. Greene, *Applied Choice Analysis – A Primer*, Cambridge University Press, New York, 2005.
[20] Brownstone, David, et al., "Drivers' willingness-to-pay to reduce travel time: evidence from the San Diego I-15 congestion pricing project", *Transportation Research A*, Vol. 37, 2003, pp. 373–387.

opposed to being used in real time only). These values increase considerably for respondents from higher-income groups. For example, the respondents with monthly income over €5,000 are willing to pay €2.96 for CCTV cameras that can recognise faces. Given that the respondents indicate disinclination towards sharing CCTV data outside their country of residence (i.e. across Europe and worldwide), the WTP estimates in this case are negative, indicating that the respondents will have to be compensated if they are to accept such data sharing.

Potoglou et al. (2010)[21] estimate the WTP for standard CCTV at UK rail premises at £2 (approximately €2.41 in 2010 prices). This value falls within our estimate range when all income groups are considered. Due to a lack of previous studies on the WTP for storage and sharing of CCTV data in this context we are unable to validate our estimates.

For the respondents from the lowest income group, the WTP for having security personnel at stations ranges from €0.30 to €0.60. Respondents indicate disinclination towards physical security checks and hence the WTP estimate is negative (although the effect and WTP for security checks involving metal detectors is insignificant). Considerably higher WTP is observed for reducing the delay in security checks. Depending on the income group, respondents are willing to pay from €1.46 to €3.28 per trip to reduce the delay by an hour. These figures are low compared to published values for travel time savings. Specifically, the recommended value of non-working time for passengers of all modes in the UK is specified as £5.08/hour (approximately €6.3/hour) in 2010 prices. The guide value of working time for rail passengers in UK appraisals is £26.86/hour (approximately €33/hour) in 2010 prices.[22] In addition, the guidance suggests one minute of average lateness to be equivalent to three minutes of journey time.[23] While these WebTAG values provide an approximate benchmark it should be noted that they are specific to the UK context and vary greatly by trip purpose, income and travel mode.

[21] Potoglou, Dimitris, Neil Robinson, Chong W. Kim, Peter Burge and Richard Warnes, "Quantifying individuals' trade-offs between privacy, liberty and security: the case of rail travel in UK", *Transportation Research A*, Vol. 44, 2010, pp. 169–181.
[22] WebTag Unit 3.5.6, *The Reliability Sub-Objective*, Department for Transport, January 2014.
[23] WebTag Unit 3.5.7, *Values of Time and Vehicle Operating Costs*, Department for Transport, January 2014.

Figure 10: Willingness to pay in the Travel context (average valuation for most countries)

2.2 Choice of an Internet Service Provider (Internet)

The Internet experiment was designed to elicit respondents' preferences concerning the storage and sharing of information on their Internet usage and the service offered by their Internet Service Provider (ISP) to improve security and privacy. Table A.2 in Appendix A shows the results from the discrete choice model describing respondents' choices from this experiment.

2.2.1 Preferences across EU27 countries

As in the preceding section on Travel, similar preferences for Internet privacy and security are observed in most countries. Again, where the preferences differ significantly in a given country these are specifically identified and the effects are presented in the charts, which can be interpreted in the same way. In this way, the preferences of respondents in a particular country can be clearly compared with those of the majority of the Member States ('all other countries').

Type of information stored

The reference level for the storage of Internet usage information is that no information is stored. As shown in Figure 11, most respondents in the EU27 dislike having any information on their Internet usage stored (values to the left of the vertical axis) and this aversion increases with the amount of data being stored. Only five countries show preferences that are significantly different. Of these, respondents in Lithuania prefer any level of data storage compared with the base level of none at all, but still prefer that a lower rather than a higher level of information is stored. Respondents in Bulgaria and Latvia also prefer that some data are stored but are still averse to higher levels of data storage, while those in Finland and Ireland generally exhibit a greater dislike of any data storage than other respondents across the EU27.

Duration of storage

With regard to preferences for how long data relating to Internet usage should be stored, there is a common response across almost all of the EU27, with only respondents in Latvia showing any difference (see Figure 12). Most respondents dislike data storage for any time period compared to the base level of data being stored for one month or less,[24] with increasing dislike for longer periods. In Latvia respondents indicate a positive preference towards storage of data for six months.

Access

There also appears to be a fairly consistent response across the EU concerning who has access to information about Internet usage (see Figure 13). Compared to a base level of no sharing of information, respondents are averse to any level of sharing and dislike more intrusive levels of access the most. In Luxembourg, there is more concern over sharing information with police departments worldwide, compared with most other countries, whereas in Slovenia there is less.

[24] The one-month level was combined with the original base level of no data storage, as its separate coefficient was insignificant and close to zero.

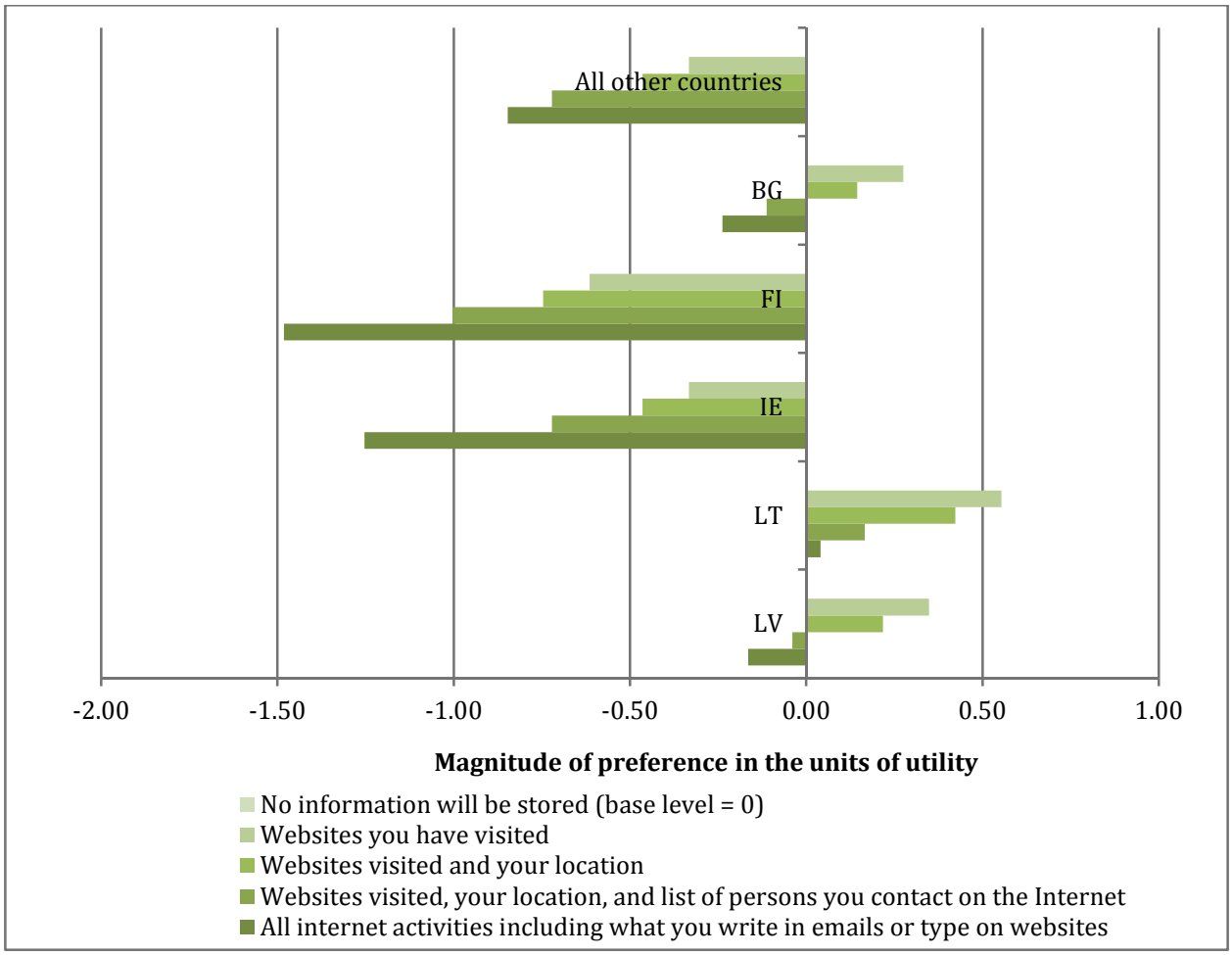


Figure 11: Relative preferences for the type of Internet information stored across the EU27

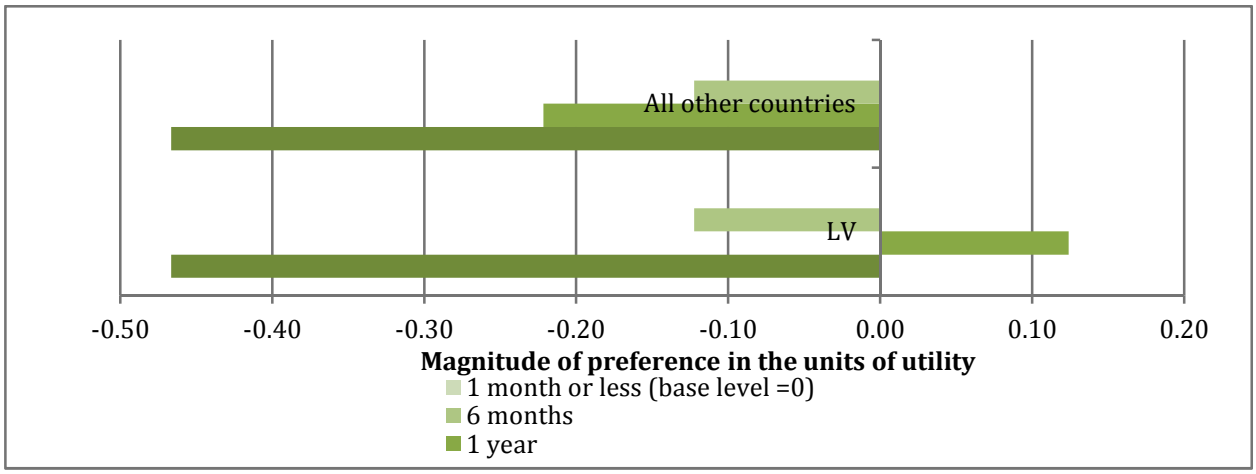


Figure 12: Relative preferences for the duration of Internet information storage across the EU27

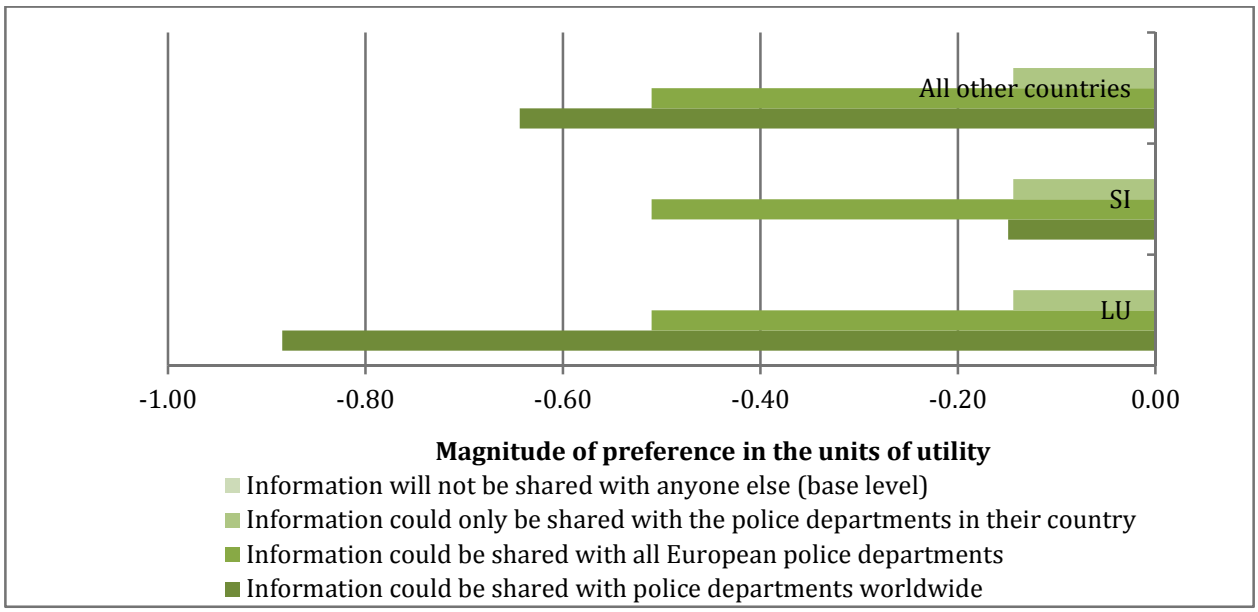


Figure 13: Relative preferences for access to Internet data across the EU27

Prerequisite for continuous surveillance of Internet users by police

The results for respondents' views on the level of surveillance of Internet users are less consistent across the EU27. On average, compared to a baseline where there is never any surveillance, respondents in all EU27 Member States prefer that surveillance takes place 'only with a warrant'. They are averse to having more intrusive levels of surveillance. As can be seen in Figure 14, respondents in Denmark and Spain differ from the EU average only in having a stronger degree of preference for the minimum level of surveillance ('only with a warrant'), while in Malta surveillance at some levels is actively preferred. Finally, for Lithuania, we see that there is a stronger aversion to higher levels of oversight of Internet users.

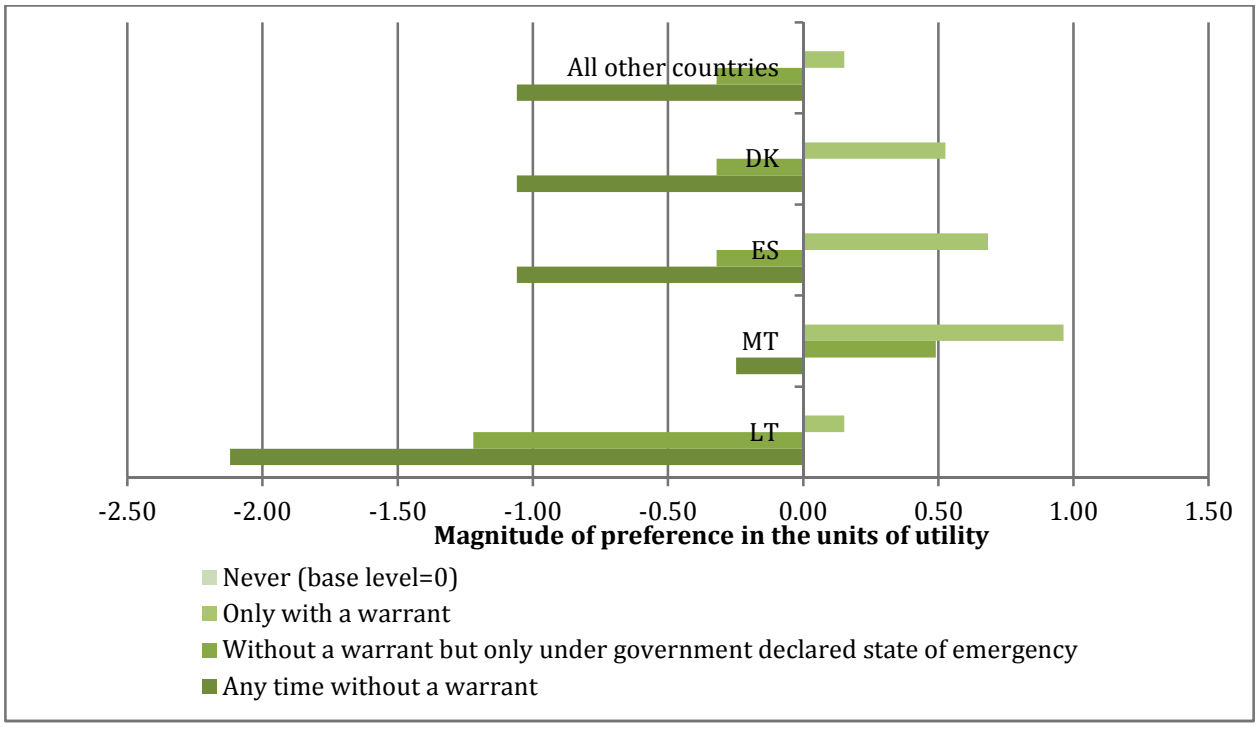


Figure 14: Relative preferences for police surveillance of Internet users across the EU27

Services offered to improve online privacy

The base level for this attribute is that an ISP will not offer any service to improve online privacy. Compared to this respondents in all countries prefer some level of service to improve their online privacy, with the strongest preference for the ISP actively hiding their information from others (see Figure 15). Respondents in Belgium and Estonia have stronger preferences than other EU countries, while those in the Czech Republic and Slovakia are mainly weaker.

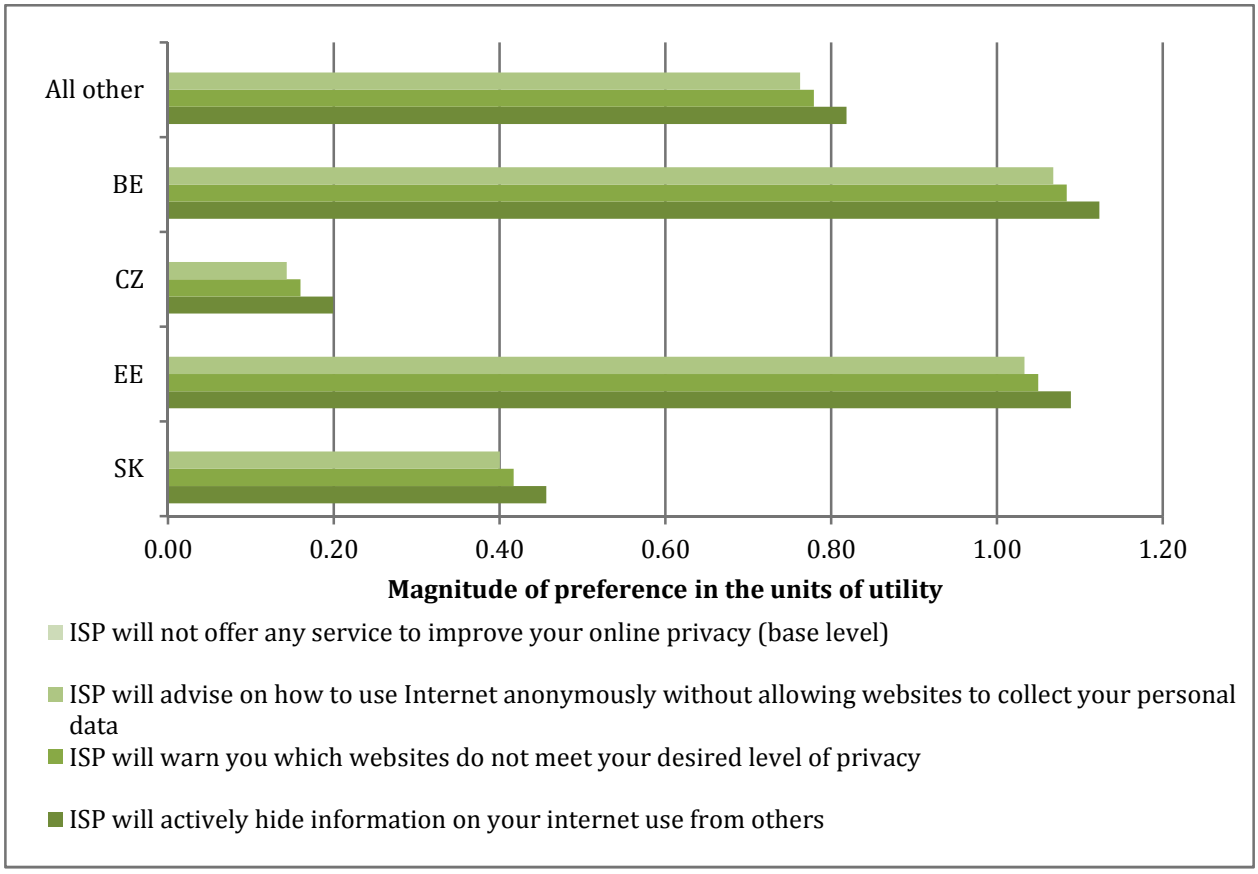


Figure 15: Relative preferences for services for online privacy across the EU27

Surcharge on top of monthly fee to pay for Internet security (cost)

Some of the experiment choices included a cost for additional Internet security. As in the Travel context, we see that households with higher incomes are less sensitive to increases in costs. Adjacent bands were again grouped when the coefficients were not statistically different for individual income bands leading, in this case, to three separate income bands in the final model (less than €500, €500 to 1,500, and greater than €5,000). A separate coefficient was estimated for those respondents who did not provide their income (responses of 'prefer not to say' or 'don't know'). Respondents in this group were further split into two groups (low-/medium- and high-income countries) to account for the wide range of average incomes across the EU27. Thus, the final Internet model contains cost sensitivities for five different population segments based on income. The estimated coefficients indicate that respondents dislike paying an additional surcharge to cover security and, as expected, the sensitivity to cost decreases with increasing income.

Reduction in monthly fee to pay for Internet security (discount)

In contrast to the Travel and Health contexts, in the Internet context participants also saw scenarios in which they were offered a discount to the monthly fee from their ISP for a certain level of service provision. This discount variable was treated in a similar way to the linear cost variable described above. In this case,

however, no significant difference in sensitivity for discounts was observed for respondents from different income levels. For respondents who did not state their incomes, tests were undertaken to understand if the discount variable could be split into different categories based on the average income of their country. The tests did not show a significant difference in sensitivity of the discount coefficient by the average income of the country. Hence only two discount coefficients are estimated in the final Internet model.

2.2.2 Differences by socio-economic status

After testing for country-specific effects we also tested effects for various socio-economic characteristics, specifically those relating to different age (18 to 24, 25 to 34, 35 to 44, 45 to 54, 55 to 64 and 65 plus), gender, working status (full time, part time, looking after family, unemployed, student, retired, not in work due to disability, seeking work, and other), education level, income, and location of residence (big city, suburb, town, village, countryside/farm). These effects are tested on all attribute levels (except on cost) and on the constant for the 'none of these' alternative. We observe the following significant effects:

- While people of all age groups across the EU27 are generally averse to any level of storage of information regarding their Internet usage, younger people (aged 18 to 24) are less averse to storage of information on the websites they have used. Females and respondents with lower secondary education are less strongly averse to all levels of information storage.
- In terms of the conditions for continuous Internet surveillance, people over the age of 65 are less averse to higher levels of surveillance than other age groups; indeed they prefer surveillance at any time without a warrant. Those in the 55 to 64 age group are, however, more concerned about police surveillance without a warrant during a state of emergency. We also found that, while people of all ages prefer some level of online privacy service, those over the age of 65 have stronger preferences.

2.2.3 Willingness to pay and willingness to accept

Following the methodology outlined in the Travel section, we can estimate willingness to pay (WTP) for services to improve privacy and security on the Internet. WTP is calculated for the service improvements using the cost coefficient for surcharges for service improvements on top of the monthly fee (see Figure 16). In addition, for the Internet context, using the discount coefficients it is also possible to estimate a willingness to accept (WTA) payment for a reduced service level for Internet privacy and security (see Figure 17). As the model is linear and all the attribute coefficients are estimated with respect to a base level (the coefficient of which is implicitly set to zero), the WTP is simply estimated as a negative ratio of the coefficient of a given attribute level to the coefficient of cost. Moreover, the cost coefficient is segregated by income group allowing the estimation of WTP for each of the income groups. By the same reasoning, the WTA is the ratio of the attribute coefficient to the discount coefficient,[25] although in this case no differentiation by income was justified and only one WTA value is presented for each attribute.

In line with the Travel results, the WTP and WTA values presented in Figure 16 and Figure 17 are representative for the majority of countries and socio-economic groups.

[25] As the discount enters the utility function as a negative cost, the WTA calculation requires a sign reversal.

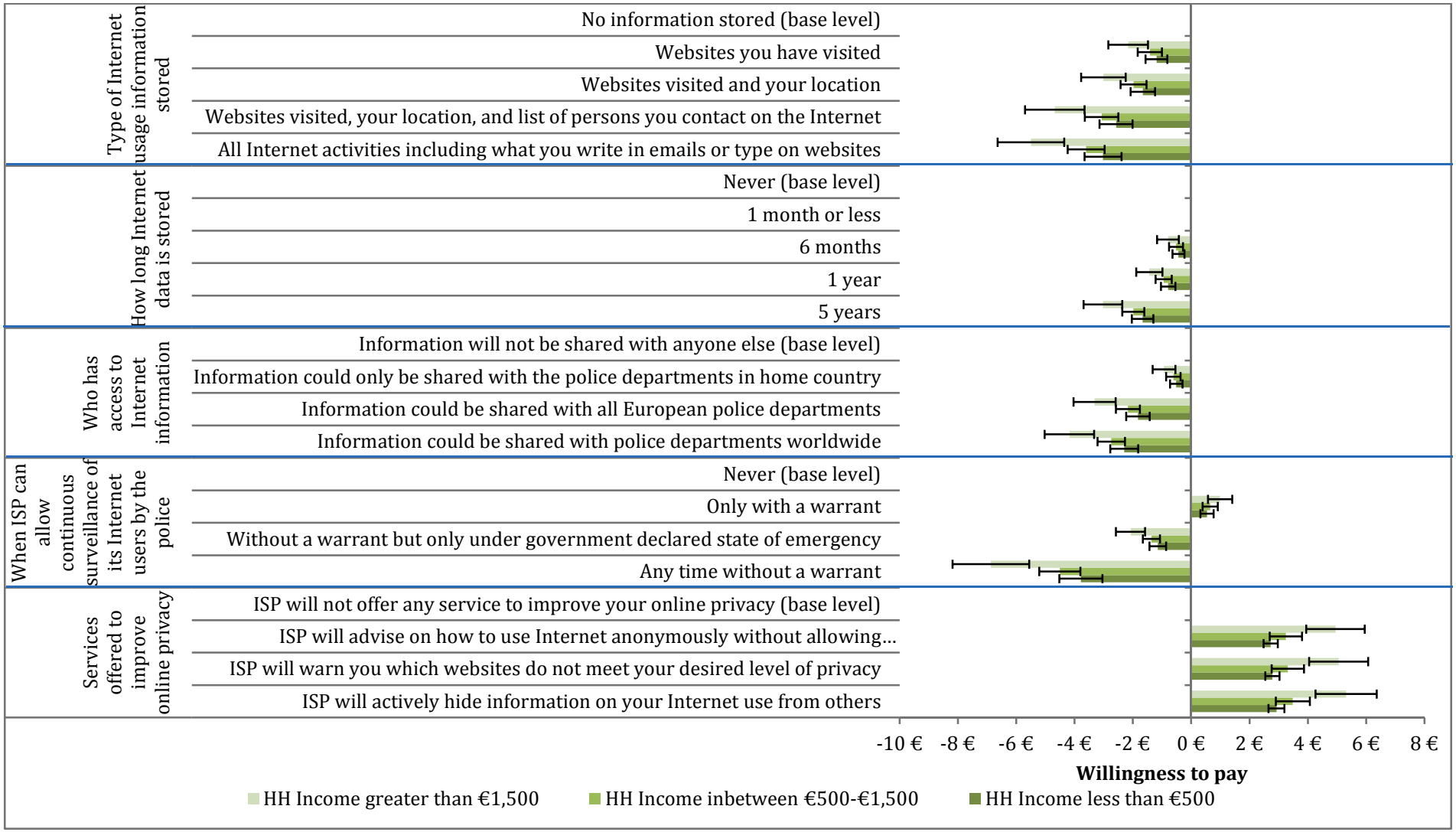


Figure 16: Willingness to pay for privacy in the Internet context (average valuation for most countries)

Of all the attributes considered in the Internet experiment, respondents are willing to pay a monthly premium for their ISP to offer them services to improve online privacy and security. Respondents in the lowest income group are willing to pay from €2.73 for the lowest level of protection up to €2.93 for the highest level. The willingness to pay increases with income; compared with households with an income less than €5000, the highest income group will pay more than €2 extra for the same level of service.

While respondents are willing to pay for services to protect them online, the results of the SP analysis show that they are also willing to trade off some of their privacy online in return for a discount on their monthly Internet fee. Thus respondents are willing to accept some degree of storage of and access to information relating to their Internet usage and, as shown in Figure 17, the greater the level of intrusion, the larger the discount that is required. Respondents appear to be most concerned about the amount of information stored rather than how long it is stored or who would have access to it. They would be willing to accept a discount in the range of €2.95 to €7.50 for increasing levels of storage of information, whereas lower discounts for duration (€1.08 to €4.13) and access (€1.27 to €5.70) would be acceptable.

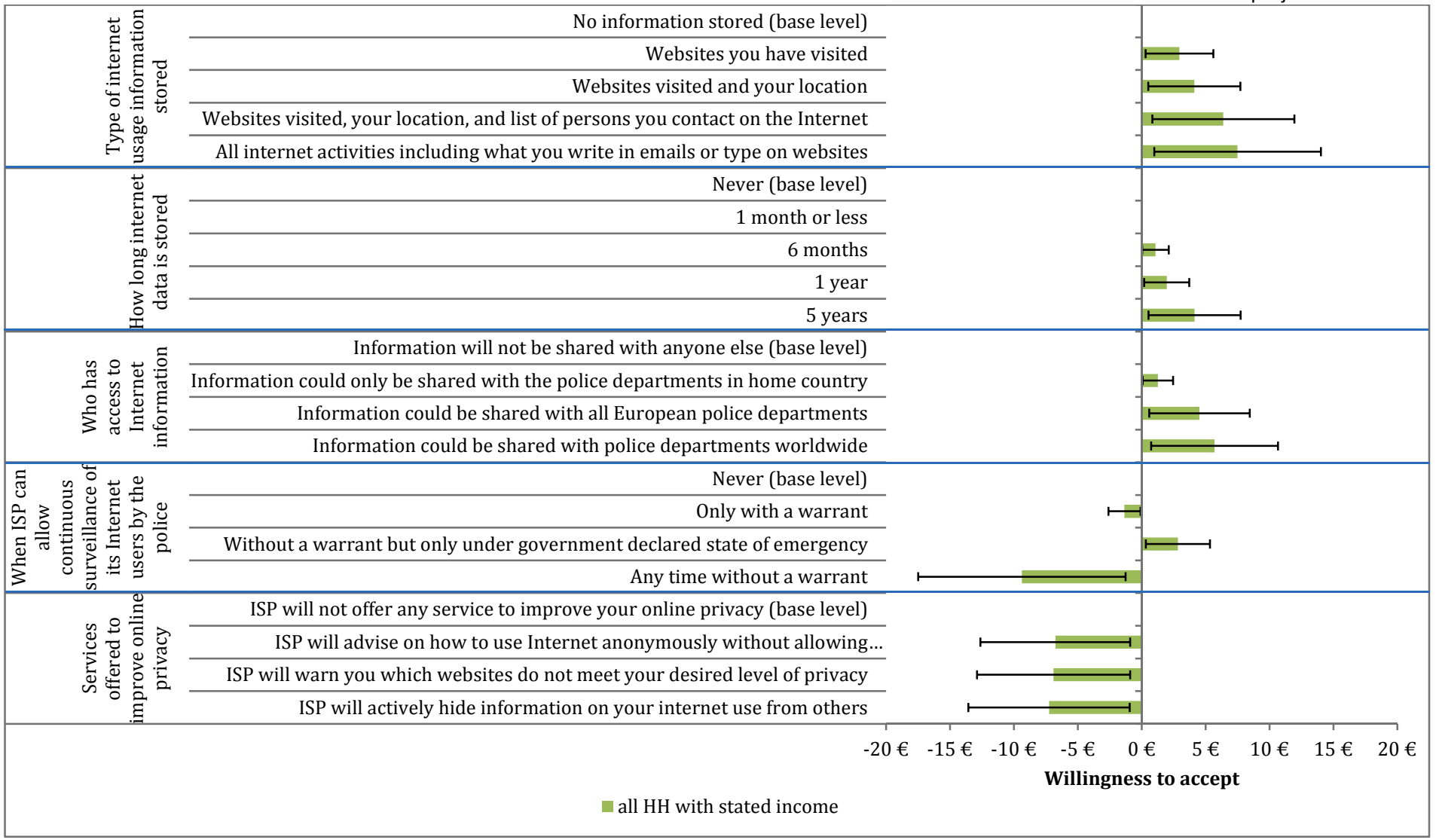


Figure 17: Willingness to accept in the Internet context (average valuation for most countries)

2.3 Choice to purchase a device/service for storing health information (Health)

The Health experiment explored respondents' preferences for data storage on devices and systems and access to health information. Table A.3 in Appendix A shows the results from the Health model.

2.3.1 Preferences across EU27 countries

In line with the Travel and Internet contexts, similar preferences for characteristics tested in the Health experiment are observed in most countries. For each attribute, preferences for those countries that differ significantly from the majority are discussed below with accompanying figures.

Information stored on a health data storage device/system

In most EU27 countries, compared to a device/system that only stores basic health status information, respondents prefer a device/system that can also store additional information relating to their identification and/or lifelong health conditions (see Figure 18). However, respondents in most countries are averse to storage of information relating to all other health conditions and medical history. Basic health status information includes information on blood groups, allergies and diabetic status. The lifelong health conditions include asthma, disabilities, cancer, etc.

Respondents in the UK indicate a stronger preference for all three types of device/system storing more than basic health information, whereas respondents in Cyprus indicate a very high preference for devices that store information relating to all health conditions and identification, as well as identification and lifelong conditions. In the Czech Republic and Lithuania, respondents indicate a disinclination towards devices that store additional information compared to devices that only store basic health status information.

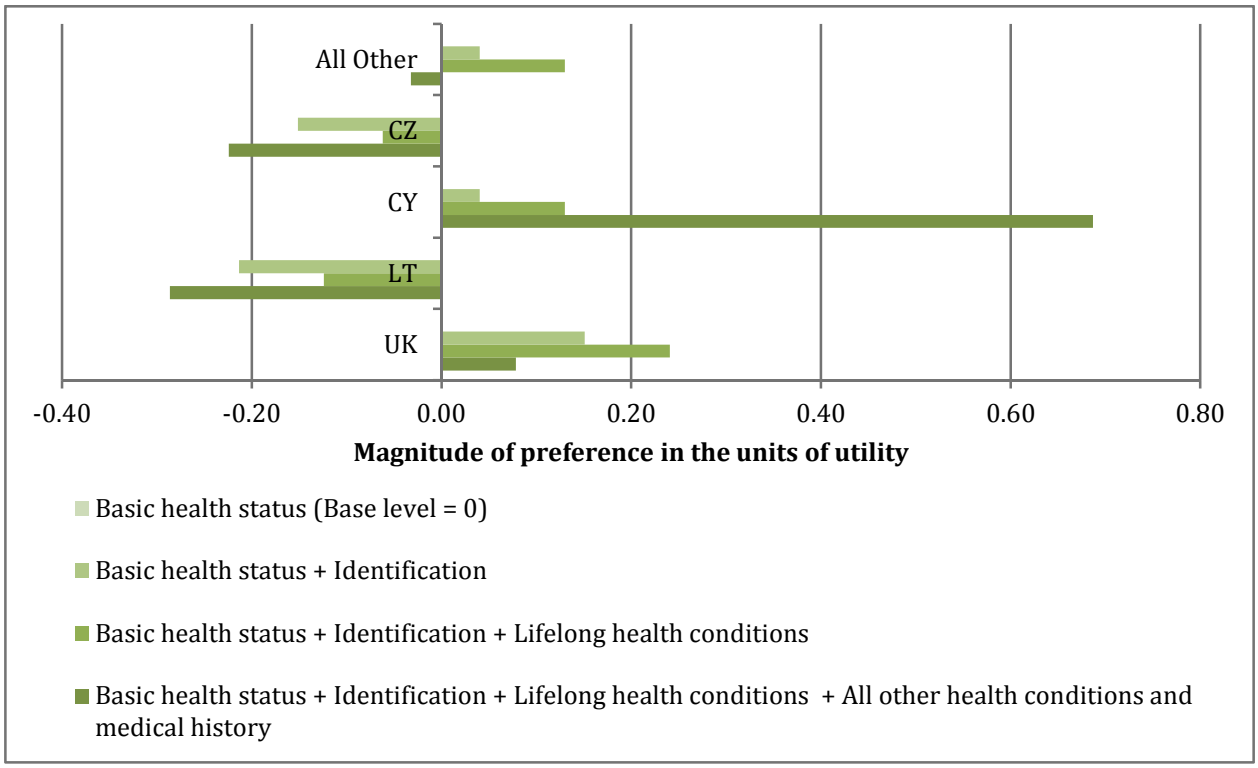


Figure 18: Relative preferences for type of information stored in the Health context

Access to information by personnel

In most EU27 countries, respondents prefer devices/systems that can be accessed by doctors and nurses, as well as paramedics (see Figure 19). However, they dislike the idea that fire and rescue personnel may also have access to the devices/systems (compared to those which provide access only to doctors and nurses).

The preference for devices with additional access only for paramedics is stronger in Estonia compared to other countries in the EU27. In Denmark respondents indicate stronger disinclination towards devices/systems with additional access for fire and rescue services. In Slovenia respondents indicate a stronger disinclination towards additional access for both paramedics and fire and rescue, preferring to keep access limited to only doctors and nurses.

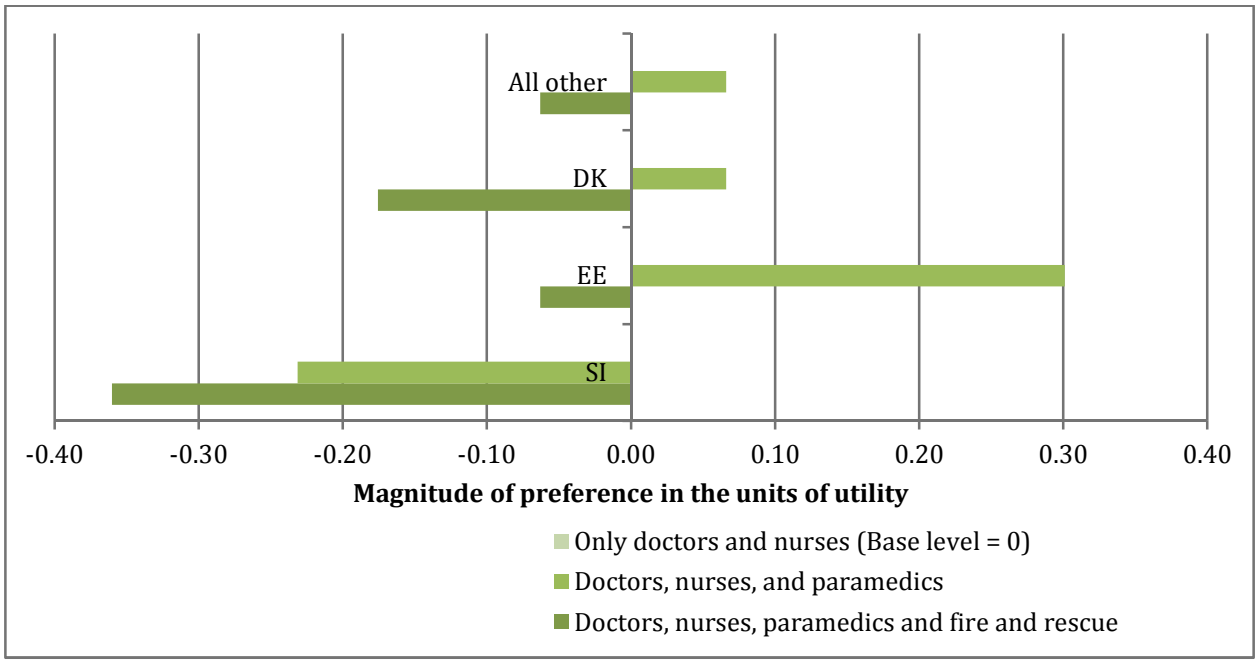


Figure 19: Relative preferences for access to health information

Access to information by country

In most EU27 countries, respondents prefer that the information stored on a device/system can be accessed across the EU rather than in their home country alone (see Figure 20). However, respondents are averse to a device/system with worldwide access to personal information compared to one that provides access only in their home country. Respondents in Belgium, Spain, Ireland and Romania indicate a preference for wider access across the EU and worldwide; however, Europe-wide access remains the most preferred option. In Austria, the Czech Republic and Slovakia respondents indicate disinclination towards the option of data sharing across Europe, and respondents from Czech Republic and Slovakia are more averse to the option of data sharing worldwide.

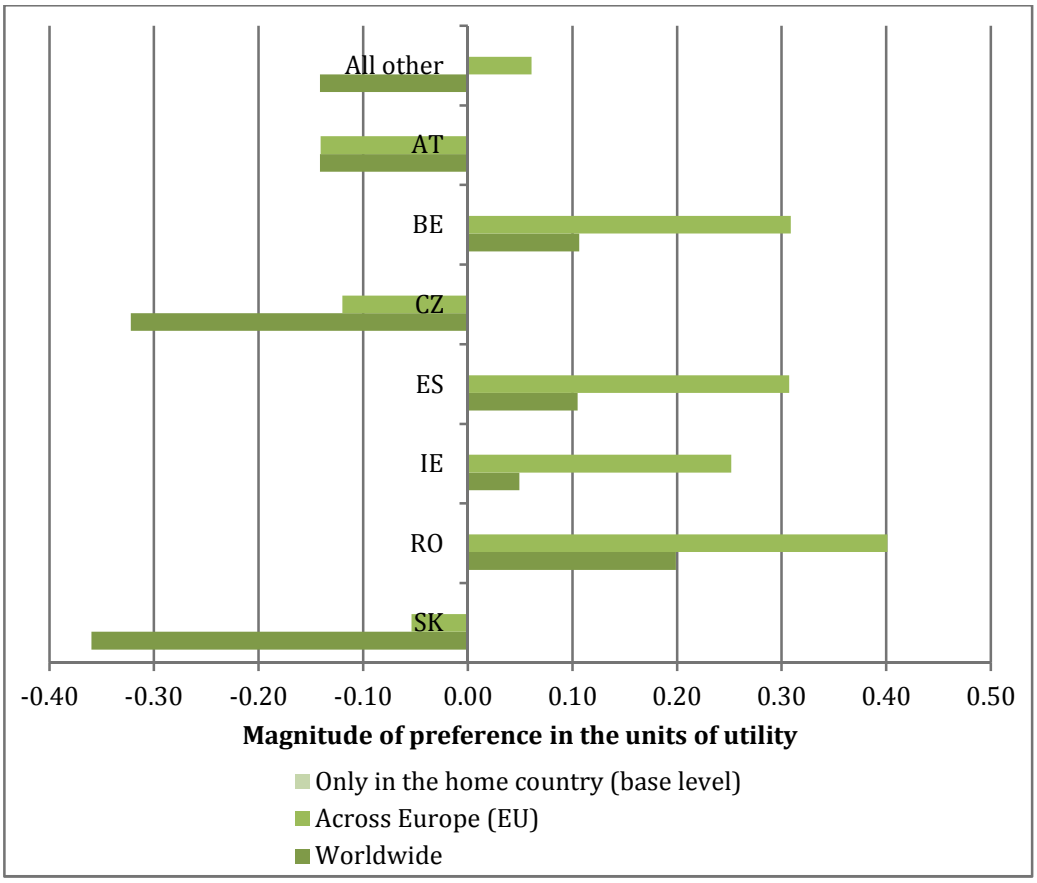


Figure 20: Relative preferences for geographic access level to health information

Viewing of health information

For this attribute, the reference level is that only a medical specialist is able to view health information. In Figure 21 it can be seen that, while in most of the EU27 countries respondents are averse to any groups other than a medical specialist having access to their data, the majority of countries exhibit different degrees of aversion for different groups, and respondents in some countries prefer that other groups are able to view their health information.

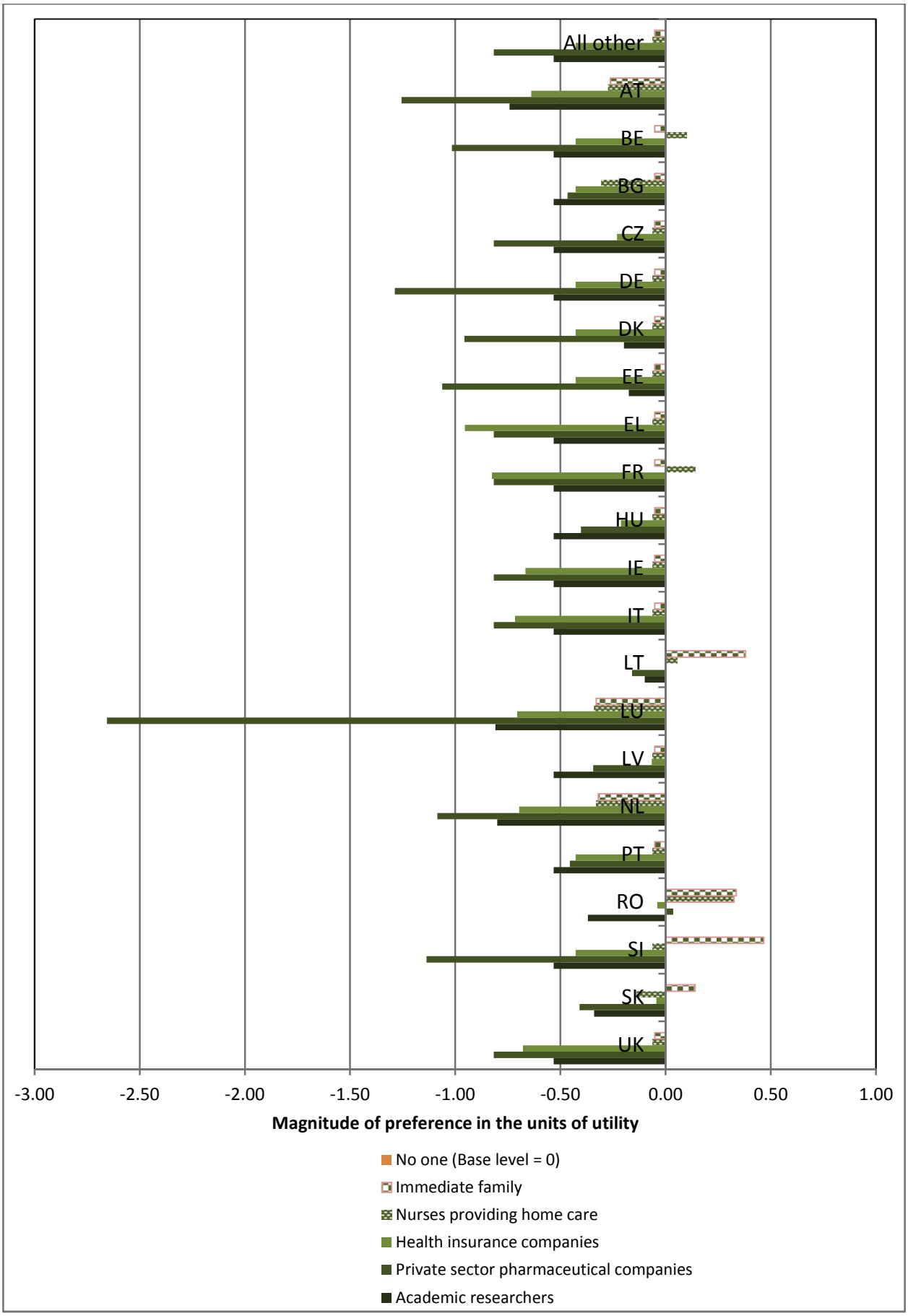


Figure 21: Relative preferences for access to health information

In general, respondents are averse to immediate family, health insurance companies, private sector pharmaceutical companies and academic researchers viewing their health information. In most countries nurses providing home care are not seen very differently compared to medical specialists (the corresponding coefficient is close to zero). In all EU27 countries respondents are averse to academic researchers viewing their health information but respondents generally have the strongest aversion to private sector pharmaceutical companies viewing the data.

In Lithuania, Romania, Slovenia and Slovakia respondents indicate a preference towards devices/systems on which information can be viewed by immediate family as well as medical specialists. However, respondents in Austria, Luxembourg and the Netherlands are more averse to such devices compared to other countries in EU27.

In Belgium, France, Lithuania and Romania respondents indicate a preference towards devices/systems on which information can be viewed by nurses providing home care, whereas respondents in Austria, Bulgaria, Luxembourg, the Netherlands and Slovakia are more averse to such devices compared to other countries.

In all but one of the EU27, respondents are averse to health insurance companies having access to health information on these devices/systems. In Lithuania respondents do not indicate a strong preference or disinclination. Respondents in Austria, Greece, France, Ireland, Italy, Luxembourg, the Netherlands and the UK indicate a stronger disinclination towards health insurance companies having access to health information.

In addition, respondents in all but one of the EU27 countries are averse to private sector pharmaceutical companies having access to their health information. Only in Romania do respondents indicate a very small preference for a device/system that can be viewed by private sector pharmaceutical companies. Of the remaining countries with specific preferences, only Bulgaria, Hungary and Latvia are more averse to academic researchers viewing their data than private sector pharmaceutical companies.

Cost

Respondents are sensitive to the additional cost per month associated with the devices/systems and they prefer a cheaper option.

When the effects are separated by respondents' monthly household income after taxes we observe decreasing cost sensitivity with increasing income. Five income bands (less than €500, €500 to 1,500, €1,500 to 3,000, €3,000 to 9,000, and greater than €9,000) are found to be required to best explain the different levels of cost sensitivity. A separate cost coefficient is estimated for the group of respondents who did not provide income data. Coefficients estimated to split the respondents with missing income by their country of residence (using low-, medium- and high-income country groups) are not statistically different. Thus only one coefficient is estimated for the respondents with missing income. Consequently, the final model contains cost coefficients for six different groups based on income. The estimated coefficients indicate that respondents dislike paying for health data storage devices/systems and, as expected, this disinclination decreases with increasing income.

2.3.2 Differences by socio-economic status

After testing country-specific effects we also tested effects for various socio-economic characteristics. We observe the following significant effects:

In general people of all age groups across the EU27 prefer devices/systems storing information relating to lifelong health conditions along with identification and basic health status. Younger respondents (18 to 24 and 25 to 34) indicate a stronger preference for devices/systems with more information. However, respondents above 34 years of age are averse to devices/systems storing information relating to all health conditions and medical history. Respondents from the youngest age group (18 to 24) are averse to any device/system on which identity-related information is the only additional information apart from basic health status (see Figure 22). Furthermore, male respondents indicate a stronger preference for a device/system that can store information on identification and all health conditions.

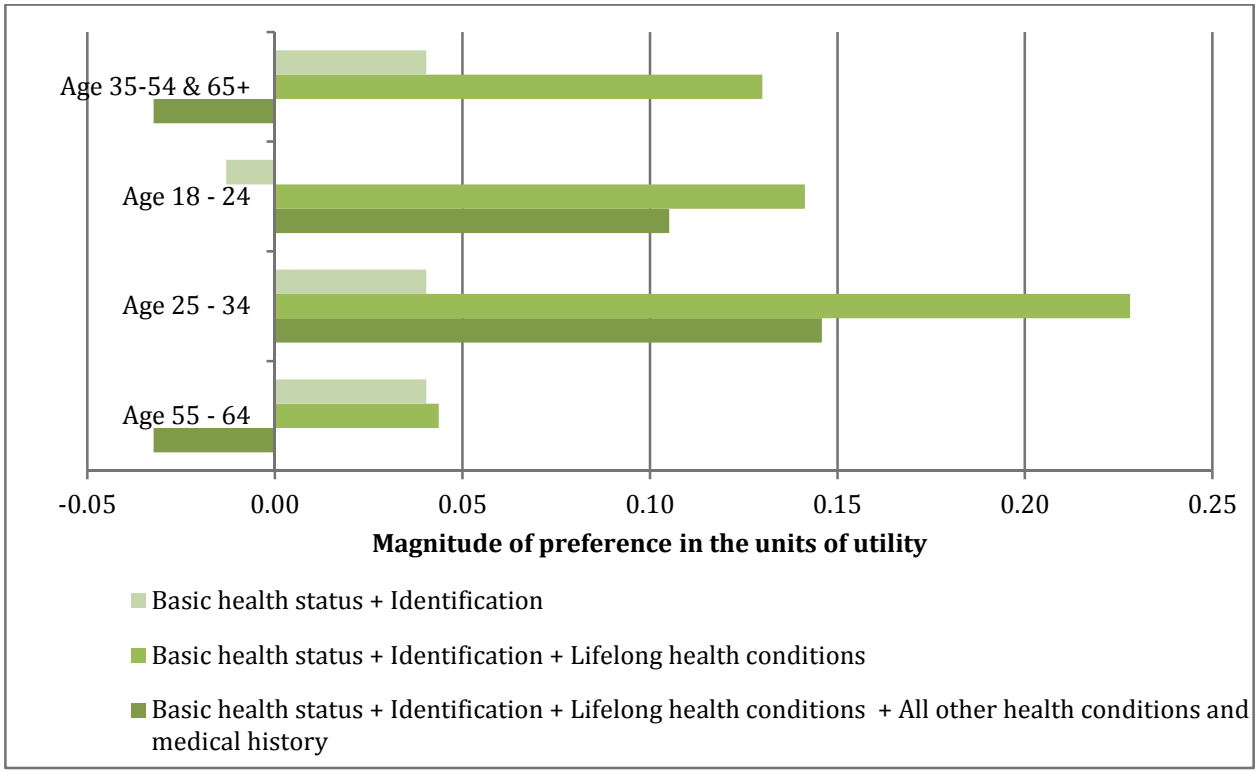


Figure 22: Relative preferences to type of information by age groups in the Health context

Compared to other age groups, respondents over 65 years old have a stronger disinclination towards devices/systems that can be accessed by fire and rescue personnel rather than doctors, nurses and paramedics.

While respondents in all other age groups prefer devices/systems that can be accessed throughout the EU (compared to access only in their country of residence), respondents over the age of 65 show a disinclination towards EU-wide access. The same group also exhibits a stronger disinclination towards worldwide access. However, younger respondents (18 to 24 and 25 to 34) exhibit a weaker disinclination towards worldwide access.

2.3.3 Willingness to pay

The coefficients for attribute levels in the Health model are used along with the cost coefficient to estimate respondents' WTP for service attributes (see Figure 23).

In general respondents are willing to pay for additional information to be stored on a device/system and the WTP increases with (monthly household) income. Respondents from the low-income group are willing to pay up to €0.31 per month for devices that can also store lifelong health conditions along with

identification and basic health information. Comparatively, these respondents are willing to pay €0.16 to widen the access to a device/system beyond doctors and nurses to paramedics, and they are willing to pay €0.14 to widen the access across the EU.

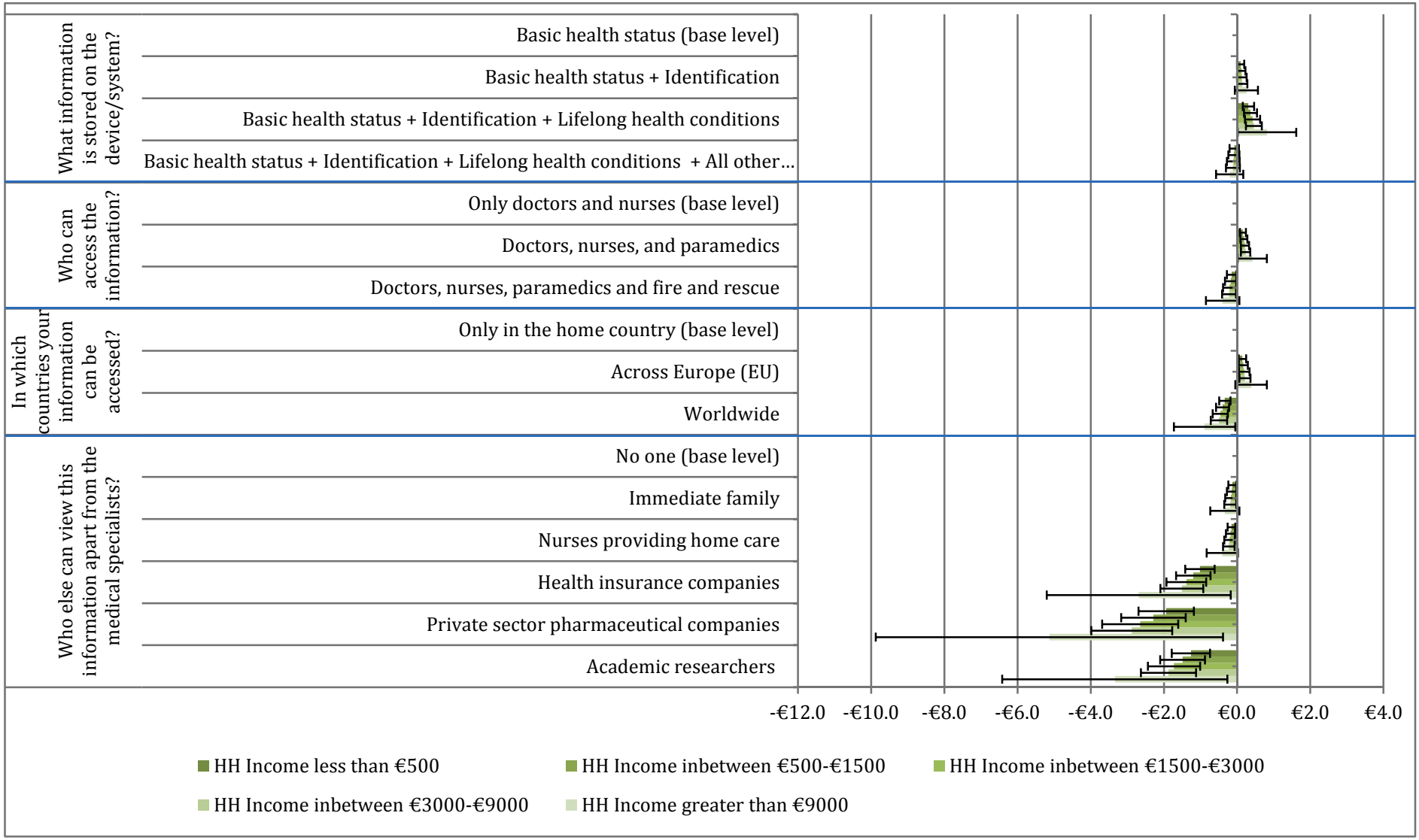


Figure 23: Willingness to pay in the Health context (average valuation for most countries)

2.4 Summary

In this section the main results presented in this chapter are summarised and compared across the contexts. It is noted that the results reflect the average preferences of individuals within a country.

2.4.1 Travel

Type of CCTV

- In all countries, we find that in general respondents prefer some CCTV surveillance and in all countries, except Sweden, the most advanced type of CCTV is preferred.
- Respondents in eleven countries exhibit different preferences and France and Sweden have the strongest positive preferences for all types of CCTV cameras.
- Females and older people have a stronger preference for CCTV surveillance.

Duration

- Most respondents prefer that CCTV data is stored for future use rather than just being used for real-time monitoring, with the exception of individuals interviewed in Greece.
- In terms of the amount of time the information is stored, an intermediate period of storage is preferred (15 days).

Access

- Respondents across the EU27 are averse to police forces outside their home country having access to CCTV data.
- Most respondents are less averse to European police having access than police worldwide.

Security personnel

- Respondents prefer the presence of unarmed security personnel to no security personnel.
- Most respondents prefer unarmed security over armed security: France and Belgium are the exceptions. It is noteworthy that police are routinely armed in these countries.
- Respondents in the UK, Hungary and particularly Germany are averse to armed private security personnel.

Security checks

- There are country-specific preferences in more than half the EU27, but most respondents are averse to any kind of security checks.
- In Belgium, France, Italy, Spain and the UK there is a preference for randomly selected people to go through a metal detector or full body scanner.
- Younger people (aged 18 to 24) are more averse to security checks.

Willingness to pay

- In the majority of countries, respondents are willing to pay for CCTV surveillance and to avoid delays due to security checks, with higher-income groups willing to pay more. WTP also depends on various country-specific and socio-economic effects identified in the Travel model. For example, males are less likely to prefer the presence of CCTV cameras and therefore would pay less than females for advanced CCTV cameras.

2.4.2 Internet

Type of information stored

- In most countries we observe that respondents prefer that information on their Internet usage is not stored, with the strongest aversion for the most comprehensive data storage levels.
- Different preferences occur in five countries; in Bulgaria, Latvia and Lithuania, some data storage is preferred over none.
- Respondents aged 18 to 24 are the least averse to having some information on their Internet usage stored rather than none.

Duration of storage

- Respondents in all countries except Latvia are averse to data being stored for periods greater than one month, with greater dislike of longer periods of storage. In Latvia, a six-month storage term is preferred.

Access

- Respondents in all countries dislike police having any access to their Internet usage data. They are least averse to access by police in their own country and, apart from in Slovenia, most averse to access by police worldwide.

Continuous surveillance of Internet use

- Respondents across the EU27 prefer that Internet surveillance takes place only with a warrant, compared to no surveillance at all.
- In most countries, with the exception of Malta, respondents are averse to any kind of surveillance without a warrant.
- Older people (>65 years) exhibit less aversion to higher levels of surveillance and prefer surveillance at any time without a warrant.

Services to improve online privacy

- Respondents in the EU27 prefer that their ISP offer services to improve online privacy and all respondents prefer most that their ISP actively hides information from other users.
- Belgium, the Czech Republic, Estonia and Slovakia exhibit different preferences for other levels of service.
- Respondents aged over 65 indicate a stronger preference for services to improve online privacy.

Willingness to pay and willingness to accept

- In the majority of countries, respondents are willing to pay for services to improve online privacy, with higher-income groups being prepared to pay more.
- In the majority of countries, respondents are willing to accept discounts for their information to be stored and accessed by police. In this case there is no differentiation by income and the largest discounts would be required for storage of detailed information and access by police worldwide.
- Respondents' WTP or WTA further depends on the country-specific and socio-economic effects identified in the Internet model.

2.4.3 Health

Type of health information stored on device/system

- Most respondents prefer health devices/systems that store identification data along with information on lifelong health conditions as well as basic health data, but are averse to devices that store more information, including information on all health conditions and medical history.
- Respondents in Cyprus and the UK prefer devices/systems with all levels of data storage, whereas the opposite effect is seen in the Czech Republic and Lithuania.
- Older respondents are averse to devices/systems that store data on all their health conditions and medical history, while younger people (<34 years) have stronger preferences for more health data to be stored.
- Males have a stronger preference for devices with more data storage.

Access to health information by personnel

- Respondents in all countries except Slovenia prefer that paramedics have access to health data on devices/systems in addition to doctors and nurses.
- All respondents are averse to fire and rescue services also being able to access health information; respondents over 65 years old show a strong disinclination for this level of access.

Access to health information by country

- Most respondents prefer that data can be accessed in across the EU and not just in the home country (Austria, the Czech Republic and Slovakia are averse to this level of access).
- Most respondents are averse to worldwide access compared to home country access only (Belgium, Ireland, Romania and Spain are the exceptions here).
- Respondents over 65 years old are averse to data being accessed outside their home country.

Viewing health information

- This is an area where we see substantial variation in the preferences of respondents across the EU27.
- Respondents in most countries are averse to information being viewed by groups other than medical practitioners; access by some groups is preferred in Belgium, France, Lithuania, Slovakia and Slovenia.
- Respondents in all countries are averse to health data being viewed by academic researchers and private sector pharmaceutical companies.

Willingness to pay

- In the majority of countries, respondents are willing to pay for devices/systems that store identification data as well as basic health data. They will pay an additional premium for data on their lifelong health conditions to be stored. Respondents in higher-income groups are willing to pay more for the same level of service.
- In the majority of countries, respondents are willing to pay for paramedics to be able to access their data in addition to doctors and nurses, and for Europe-wide access to their data rather than only in their home country.

2.4.4 Comparison across contexts

As is clear from the preceding sections, different attributes are relevant in determining how individuals view their privacy, surveillance and security in the three settings that have been considered in this study. The findings are summarised and compared across similar dimensions in Table 1. We emphasise that these findings represent the averages within countries and do not necessarily apply to individual respondents.

Table 1: Comparison of main findings from the stated choice modelling exercise

	Travel	Internet	Health
Collection of personal data	Prefer presence of CCTV to no CCTV, prefer advanced cameras	Dislike storage of data on Internet usage	Prefer devices/systems that store data on identification in addition to basic health data
Storage of personal data	Prefer storage of CCTV data for future use rather than real-time monitoring only	Dislike storage of data on Internet usage for more than one month	N.A. (data are always stored for future use)
Geographic access to data	Dislike access to CCTV data by police outside their home country	Dislike access to Internet usage data by police	Prefer access across the EU rather than in home country only
Access by personnel	Prefer presence of unarmed security personnel to no personnel	N.A. (such an attribute was not included in the scenarios)	Dislike that their health information is viewed by groups other than medical practitioners Prefer access to devices/systems storing data by paramedics in addition to doctors and nurses Dislike access by fire and rescue services in addition to the above
Willingness to pay	Willing to pay for CCTV cameras (€1.12 to €2.96 surcharge per trip) and security personnel (€0.30 to €0.94) Willing to pay to avoid delays due to security checks (€1.46 to €3.28 surcharge per hour)	Willing to pay for services to improve online privacy (€2.73 to €5.33 monthly premium) Willing to accept a payment for data to be stored (€2.95 to €7.50 monthly discount) or be accessed by police	Willing to pay for devices/systems that store more than basic health data (€0.31 to €0.80 monthly premium) Willing to pay for access to data by paramedics and across Europe
Country specific effects	In most countries the preferences align similarly	In most countries the preferences align similarly	In most countries the preferences align similarly
Socio-economic effects	Older people (>65) prefer CCTV surveillance, younger people (18–24) are averse to security checks	Younger people (18–24) are least averse to some data storage, older people (>65) are less averse to surveillance and prefer more services for online privacy	Older people are generally more averse to data being stored, while younger people (<34) are more open to it

For all three contexts, respondents were asked about their preferences for the type of data that could be stored. In the Travel context this was CCTV footage and for Health this involved devices/systems that store health-related information. In both these cases there is a strong preference for some level of data storage (and a corresponding willingness to pay for these services). This contrasts with the Internet context, where respondents are strongly averse to any information being stored. And in the same context, respondents are averse to any access by police to their data and they would require a substantial reduction in costs by providers (it should be noted that the survey fieldwork was conducted in the months following the revelations of secret surveillance programmes). Respondents are slightly less averse to some limited data access in the Travel context and, for Health, wider access is preferred as long as this is restricted to the medical profession. Surveillance was considered an important attribute in the Travel and Internet contexts and, in both cases, respondents preferred some level of surveillance to none. For the Travel context, the use of CCTV is itself a form of surveillance in addition to the presence of security personnel.

It is difficult to compare WTP between the Travel, Internet and Health contexts, as WTP in the Travel context is measured relative to the additional price per trip, whereas in the Internet context the additional cost is per month. However, it appears that respondents are much more willing to pay to protect their online information than they are to pay for increased storage of their health information.

Country-specific preferences appear to be more significant in the Travel and Health settings. A wide range of countries exhibit these effects, depending on the attribute in question, and no particular group of countries predominates. With regard to socio-economic effects, on the other hand, younger respondents generally are open to storage of data (and hence less privacy) but are more averse to surveillance, while older people exhibit the opposite preferences. These findings hold in all three contexts. Other socio-economic factors, such as education level, are not found to play an important role in distinguishing preferences; gender effects are also limited. One exception is in the Internet context, where respondents with an education attainment at the lower secondary level are less averse to higher levels of data storage.

3. The role of attitudes in determining the preferences relating to security, surveillance and privacy

While the models developed in Chapter 2 take into account the differences in preferences according to respondents' country of residence and socio-economic characteristics, they could be further extended to include respondents' attitudes. Respondents' attitudes towards privacy, surveillance and trust can have a significant impact on their preferences.[26] The PACT survey presented respondents with statements designed to capture their attitudes relating to trust in the government, general distrust, risk taking, privacy concern in each context and concerns relating to surveillance. A summary of the effect of adding attitudes to the choice models is provided in this chapter. We also investigate how socio-economic factors influence average attitudes. The socio-economic influences included in this study should enable identification of the population segments of interest and will be particularly useful for the next work package (WP5), which will develop the Privacy Reference Framework. In recent studies these two steps of linking attitudes and preferences are combined in more advanced forms of models frequently referred to as Integrated Choice and Latent Variable (ICLV) models. ICLV models incorporate latent variables relating to attitudes and preferences in a single model specification and can offer a richer understanding of both attitudes and behaviour. However, given the size of PACT dataset it was not possible to develop ICLV models within project timescales, as ICLV models take multiple days to converge. We have therefore used a two-step method in which we first estimate a discrete choice model with responses to attitudinal indicators (manifest variables) and then estimate a structural equation model to understand the link between attitudinal indicators and socio-economic factors. The model used in the first step can be referred to as a reduced form model and it does not necessarily provide a poorer fit to the data compared to the ICLV model.[27]

3.1 The effect of attitudes on preferences

Attitudes and perceptions are latent constructs or abstract psychological concepts. These cannot be measured directly and can only be observed indirectly by their effect on the manifest variables; in this study these are statements to which respondents are asked to indicate their agreement on an ordinal scale (in this case from 1 to 5). Appendix B (Table B.1) describes the statements (manifest variables) used to capture the latent constructs around trust, risk taking and a general surveillance-related concern. The statements designed to capture the general surveillance-related concern are about effectiveness, the motivation for surveillance and potential misuse of the surveillance measures.

Using structural equation models (described in detail in Section 3.2) we investigate the level of association between three latent constructs: general distrust, trust in institutions, and risk taking. We find that trust in institutions and risk taking is highly correlated with general distrust. The correlation coefficients are -0.82 and -0.82 for both pairs, indicating that high (general) distrust is associated with lower trust in institutions and lower risk taking. Thus we use general distrust as a proxy for the other two latent constructs in the discrete choice models in the three contexts, in order to simplify the analysis. Besides general distrust, we also include attitudes towards privacy concerns, which are captured by context-specific privacy concern questions (see Appendix B, Table B.2).

[26] Daly, Andrew, Stephane Hess, Bhanu Patruni, Dimitris ,Potoglou and Charlene Rohr, "Using ordered attitudinal indicators in a latent variable choice model: A study of the impact of security on rail travel behaviour", *Transportation*, Vol. 39(2), 2012, pp. 267–297.

[27] Daly, Andrew, and Stephane Hess, "Workshop report: latent reality", in Matthew J. Roorda and Eric J. Miller (eds.), *Travel Behaviour Research*, IATBR, 2013.

Moreover, in the Internet context a latent construct to capture attitudes to the effectiveness of online security and, in the Health context, one that captures attitudes towards the usefulness of health data storage, are also included (see Appendix B, Table B.2 for list of context-specific latent variables).

The responses to statements (manifest variables) relating to general distrust together with those specific to concerns in the different contexts are incorporated in the choice models to help explain respondents' choices in the experiments. The sub-sections below discuss the findings from the extended discrete choice models in each of the contexts. The manifest variables are used as linear terms in the choice models, taking values from 1 to 5. As these variables interact with all levels for a given attribute, the interpretation becomes difficult. Thus only selective interactions (strongly agree, neutral, strongly disagree) are presented in the following sections. Furthermore, when there is more than one manifest variable interacting with a given attribute level we keep them at the neutral level when presenting the effect due to variation in a selected variable.

3.1.1 Travel

The manifest variables capturing general distrust, general attitudes towards surveillance and Travel context privacy concern are tested for their effect in the Travel context discrete choice model. These tests involve investigating whether the manifest variables affect the preferences for the alternatives of presence of CCTV cameras, security personnel and physical security checks. In addition, the effect of manifest variables on preference for the alternative 'none of these' is also tested. The statistically significant findings are listed below. The full model results are presented in Appendix B (Table B.3).

Effect on preference for CCTV cameras

As expected, respondents who are more concerned about the misuse of CCTV cameras and travel data indicate weaker preferences towards CCTV cameras (see Figure 24). In contrast, those who are more concerned about misuse of security measures for sexual or racial harassment indicate a preference for the presence of CCTV cameras. It is possible that this group sees CCTV cameras as a deterrent against such harassment.

Furthermore, respondents who agree with the statements 'Often security is used as an excuse to impose stricter surveillance and control over the population' and 'Increasing surveillance increases the risk of discrimination', indicate a disinclination towards the presence of CCTV cameras.

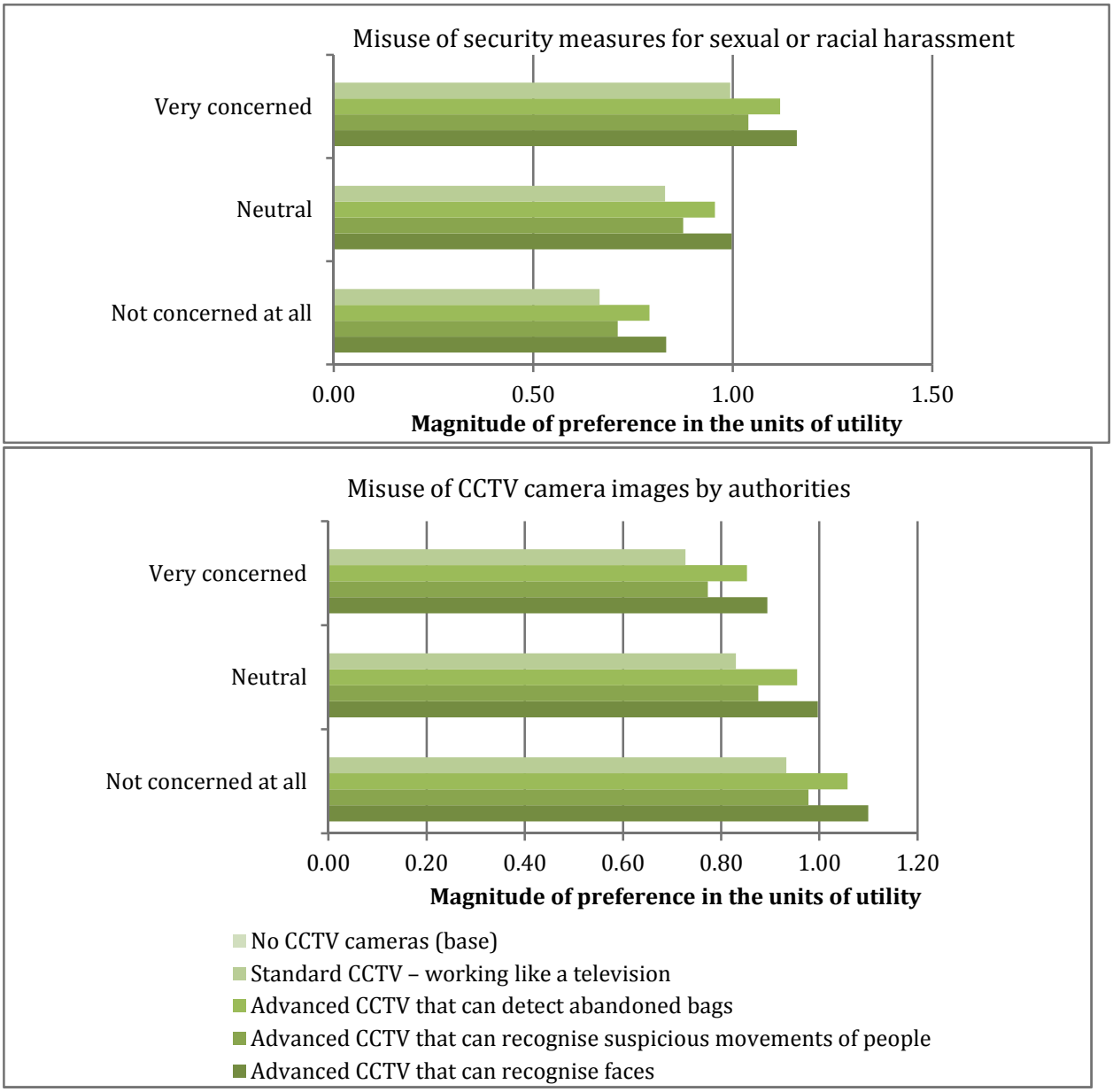


Figure 24: Effect of privacy concern on preference for CCTV cameras

Effect on preference for security personnel

Respondents who are more concerned about misuse of travel data for tracking a person's whereabouts also indicate weaker preferences towards the presence of security personnel (see Figure 25).

Figure 25: Effect of privacy concern on preference for presence of security personnel

Effect on choice making

Those respondents with higher distrust (as indicated by answers to the statements a, b, c and d on 'General Distrust' in Appendix B, Table B.1) are more likely to reject the alternatives presented in the Travel choice scenario (alternatives 'A' and 'B'), exhibiting a preference for the 'none of these' alternative. Thus respondents with higher distrust are more likely to reject any configuration of security and surveillance measures presented in the Travel context. Those who question the effectiveness of and motivation for the surveillance measures and anticipate their potential misuse are also more likely to reject both configurations in alternatives A and B and show a preference for the 'none of these' alternative.

3.1.2 Internet

The manifest variables capturing general distrust, concern for privacy and concern for security in the Internet context are tested for their effect in the discrete choice model. These tests investigate whether the manifest variables affect the preferences for all attribute levels. In addition, the effect of manifest variables on preference for the 'none of these' alternative is also tested. The main findings are discussed below, and the full model results are presented in Appendix B (Table B.4).

Type of information stored

In responding to the statements relating to concern about privacy in the Internet context, those who expressed the most concern generally have a stronger aversion to information on their Internet usage being stored than those who showed no concern at all. This result is illustrated below for the statement 'Internet usage information shared with third-party websites or companies' (see Figure 26). In this case, respondents who are not concerned at all in fact prefer some data storage. Where attitudes towards online security are concerned, respondents remain averse to all levels of data storage, with more-concerned

respondents showing greater dislike. However, it should be noted that there were some counter-intuitive results. Answers to the statements 'Personal information is not handled in a legitimate way' (privacy) and 'Technology has almost got out of control' (distrust) indicate that those with a higher level of concern were less averse to all levels of data storage.

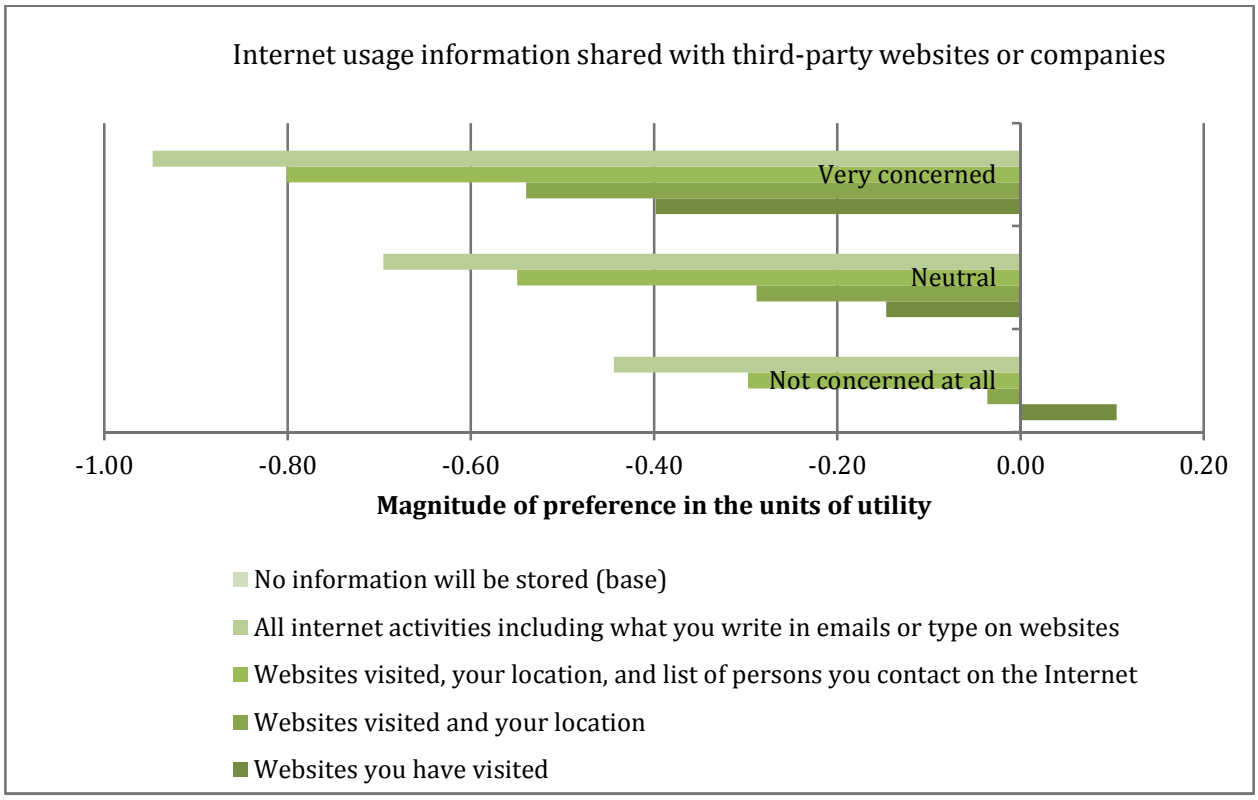


Figure 26: Effect of manifest variable for privacy concern on preferences for storage of information on Internet usage

Level of surveillance of Internet users by police

Respondents show a preference for all types of surveillance (with or without a warrant, in emergencies and otherwise). The more concerned the respondent, the stronger the preference for surveillance. This contrasts with the results without attitudinal effects (see Section 2.2), where respondents are averse to levels of surveillance other than 'only with a warrant'. An example is presented in Figure 27 and the results carry over to the other manifest variable statements. This seemingly counter-intuitive finding could be explained if respondents believe that continuous surveillance can somehow be a deterrent for unauthorised sharing of data with third parties. This finding is also similar to evidence in the Travel context that implies that respondents who have higher concern for misuse of security measures for harassment also indicate a higher preference for advanced CCTV cameras (surveillance).

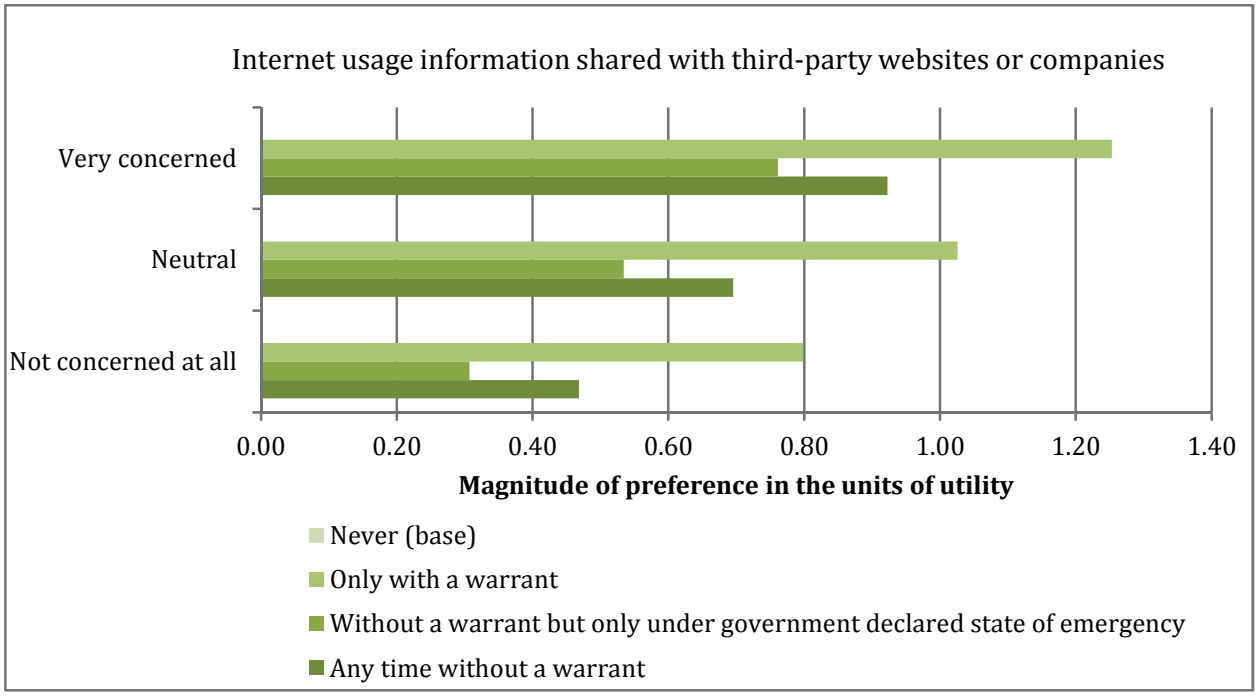


Figure 27: Effect of manifest variable for privacy concern on preferences for police surveillance of the Internet

Services to improve online privacy

Respondents who have strong concerns for online privacy have stronger preferences for all types of services to improve online privacy compared to those who are less concerned. For example, the results for the manifest variable 'Internet usage monitored by police departments in other countries' are shown in Figure 28.

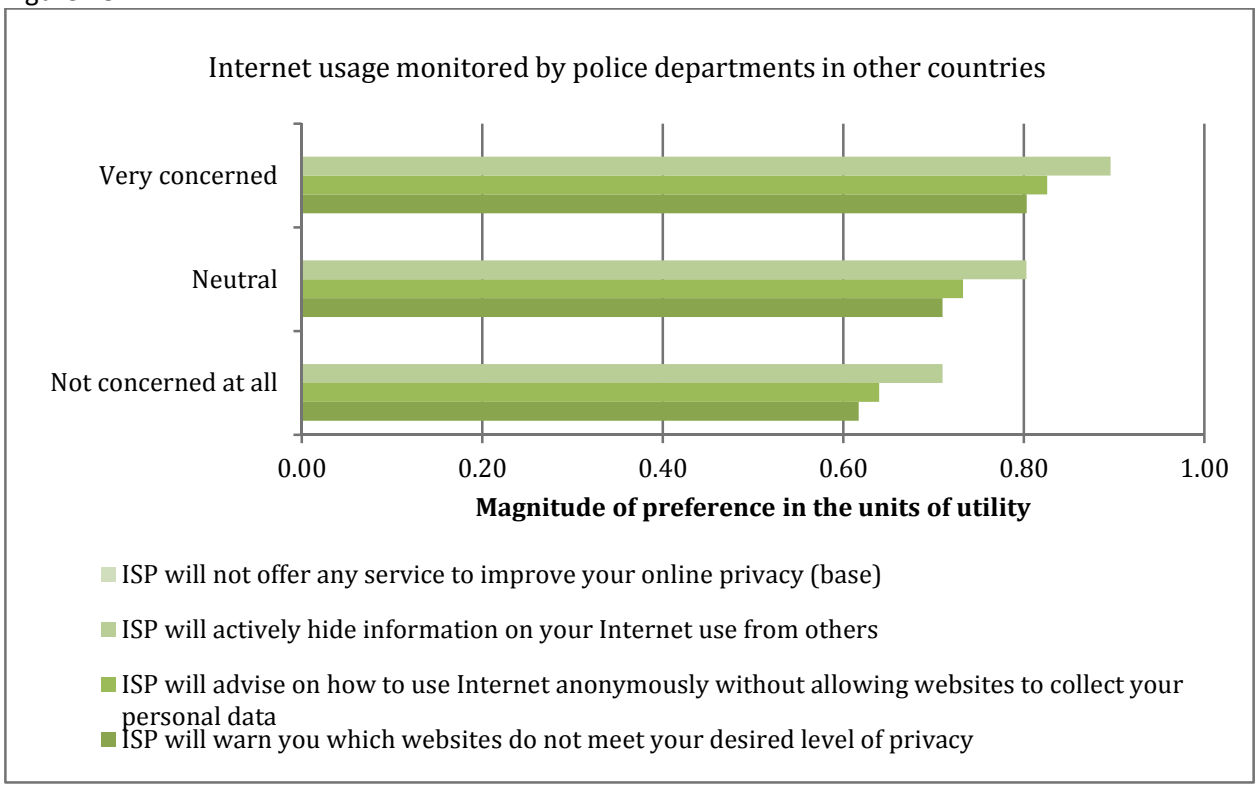


Figure 28: Effect of manifest variable for privacy concern on preferences for services to improve online privacy

For this attribute, respondents' concern for online security, as manifested by their response to the statement 'Not using services is preferable to having personal information collected and monitored online', has a slightly different effect on preferences. Very concerned respondents, i.e. those who strongly agreed with this statement, exhibit a stronger preference for being warned about websites that do not meet the desired level of privacy (see Figure 29).

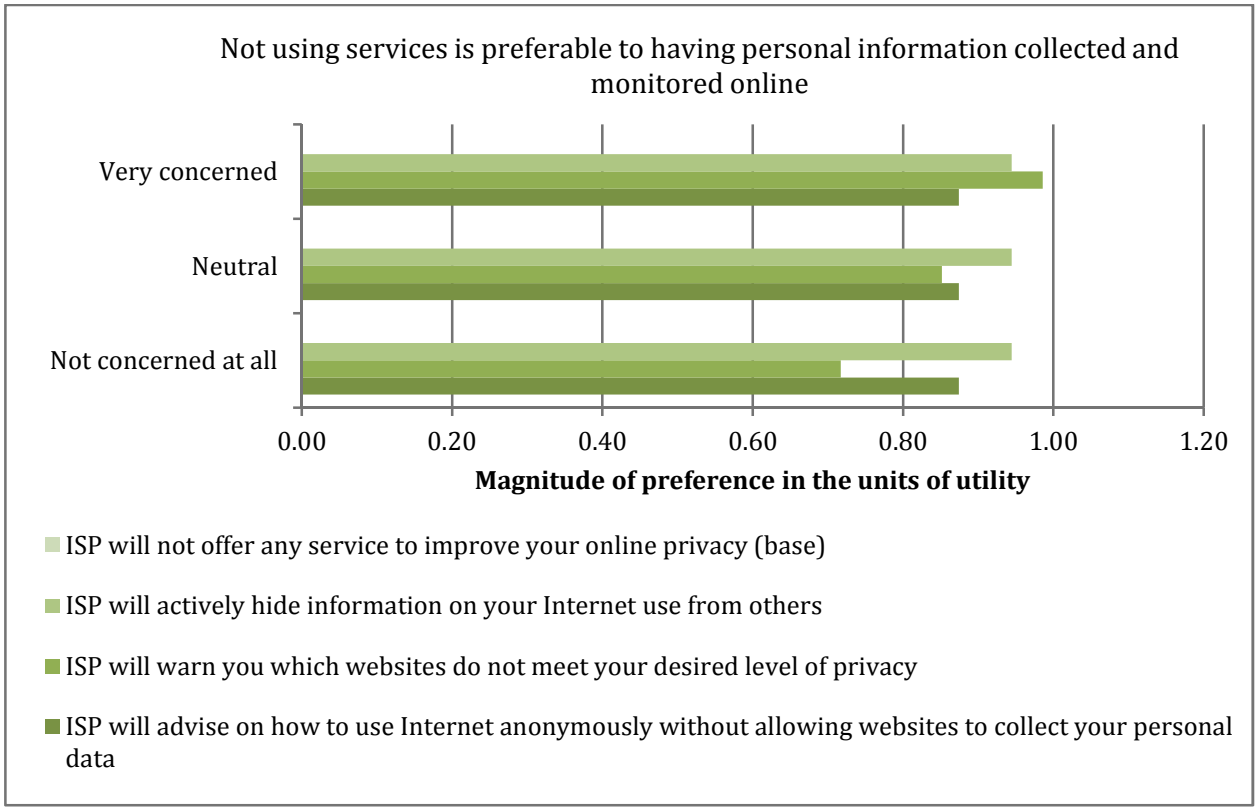


Figure 29: Effect of manifest variable for security concern on preferences for services to improve online privacy

Effect on choice making

Respondents who showed concern for privacy when using the Internet are more likely to reject alternatives A and B and choose the 'none of these' option. This indicates that none of the combinations of attribute levels presented to them in the choice scenarios provided a sufficient level of privacy. Similarly, those who exhibited a high level of general distrust or a low level of agreement with the effectiveness of online protection (i.e. they are concerned about online security) are more likely to choose the 'none of these' option.

3.1.3 Health

The manifest variables capturing general distrust, the Health context privacy concern, and the perception of usefulness of a health data storage device/system are tested for their effect in the discrete choice model. The significant findings of the tests, which involve investigating whether the manifest variables affect the preferences for all attribute levels, as well as for the 'none of these' alternative, are presented below. The full model results are presented in Appendix B (Table B.5).

Information stored on a health data storage device/system

As shown in Figure 30, respondents who are more concerned about their personal information (name, address, health conditions) being accessed by private companies (such as pharmaceutical and insurance

companies) without their consent, indicate a weaker preference towards a device/system with more information stored on it.

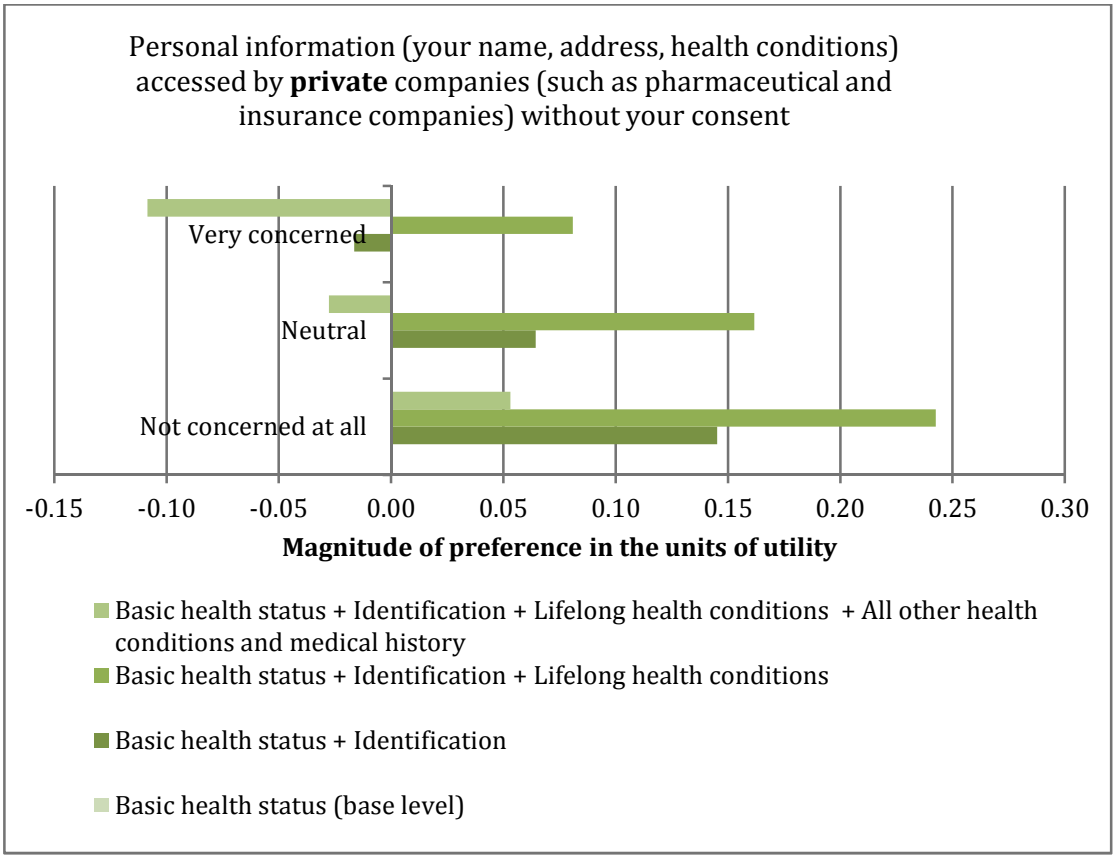


Figure 30: Effect of privacy concern on preference for information stored in the Health context

Access to the information by personnel

Respondents who are more concerned about their personal information (name, address, health conditions) being accessed by non-medical personnel (e.g. police) without their consent, indicate weaker preferences for widening access to paramedics. These respondents are also more averse to widening the access to include fire and rescue personnel.

Those who are more concerned about the misuse of personal information for harassment based on race, health status, sexual orientation, etc., exhibit both a stronger preference for widening access to paramedics and a weaker disinclination towards widening access to include fire and rescue personnel (see Figure 31). It is possible that the response to this statement is confounded with other factors such as a person's health status, which is likely to affect the preferences. For example, respondents with existing health conditions may have strong concerns relating to the misuse of information for harassment, while they are also likely to indicate preference towards wider access to information by paramedics.

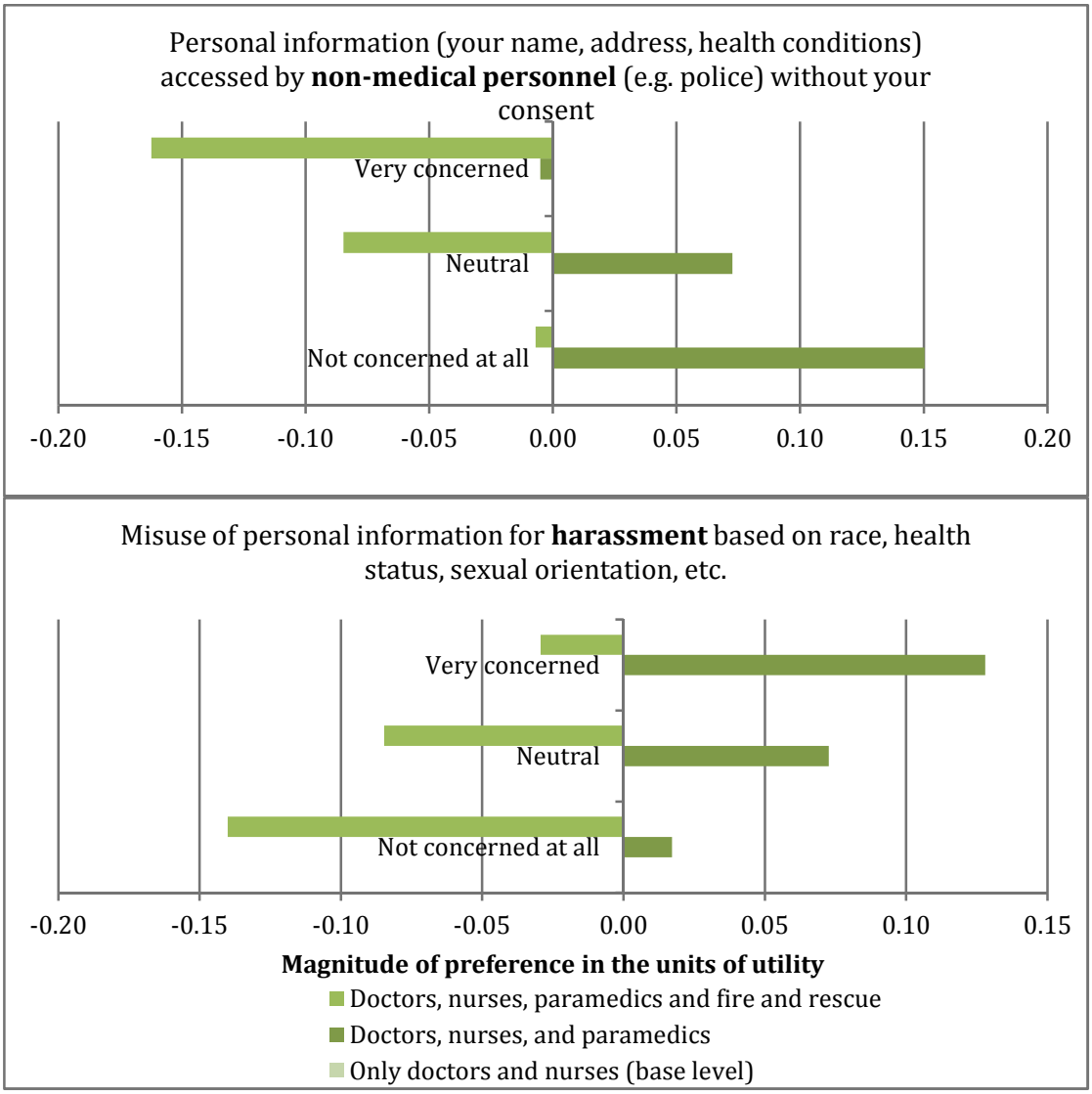


Figure 31: Effect of privacy concern on preference for access by personnel

Access to the information by country

Respondents who are more concerned about their personal information being accessed by private companies and by non-medical personnel without their prior consent show stronger preferences for wider access to health information across the EU and worldwide. This finding seems counter-intuitive.

Viewing of health information

Respondents who are more concerned about their personal information (name, address, health conditions) being accessed by private companies (such as pharmaceutical and insurance companies) without their consent, indicate a stronger disinclination towards academic researchers, private sector pharmaceutical companies, health insurance companies, nurses providing home care, and immediate family being able to view information on a device/system (see Figure 32). However, those who are more concerned about their personal information being accessed by non-medical personnel are less averse to such a device/system. It is possible that while answering this statement, respondents could be mainly thinking about police in the context of non-medical personnel, as possibly implied by the phrase 'non-medical personnel (e.g. police)'.

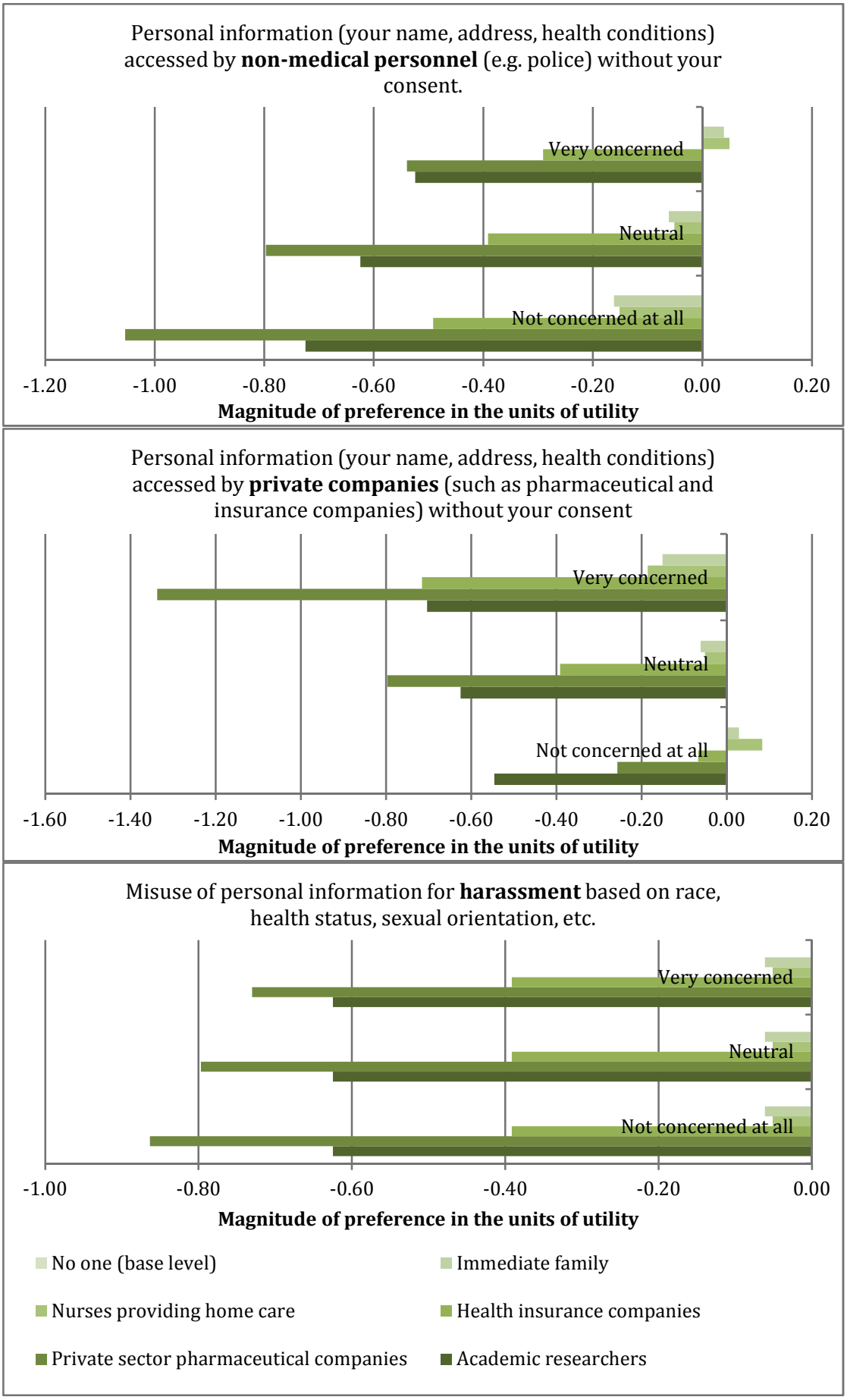


Figure 32: Effect of privacy concern on preferences for viewing of health information

Respondents who are more concerned about misuse of personal information for harassment based on race, health status, sexual orientation, etc., show a weaker disinclination towards private sector pharmaceutical companies. This finding is also counter-intuitive.

Effect on choice making

Respondents with higher levels of general distrust are more likely to reject the hypothetical health device alternatives A and B and indicate a preference for the 'none of these' option. This finding supports the view that respondents who are more distrustful are more likely to reject any configuration of the amount of data stored, level of access and cost level presented in the Health context.

Those who are more concerned about their personal information (name, address, health conditions) being accessed by non-medical personnel (e.g. police) and private companies without their consent are also more likely to reject alternatives A and B in the health device/system choice scenario and prefer the 'none of these' option. On the other hand, respondents who have concerns about misuse of personal information for harassment based on race, health status, sexual orientation, etc., are less likely to reject alternatives A and B. These findings appear counter-intuitive.

Respondents who indicate a higher level of agreement with the statement 'Healthcare providers (such as hospitals and health insurance companies) are successful in preventing unauthorised access to personal information' are less likely to reject alternatives A and B. Where a somewhat opposite view is expressed through a higher level of agreement with the statement 'I'm concerned that healthcare providers (such as hospitals and health insurance companies) are collecting too much personal information about me', respondents are more likely to reject alternatives A and B and exhibit a preference for 'none of these'.

Thus, overall, greater distrust or concern for privacy among respondents suggests that they are less likely to be satisfied with the combination of attributes proposed in the choice modelling alternatives.

Finally, turning to the issues relating to the usefulness of such devices/systems, respondents who express a higher level of agreement with the three statements below are more likely to reject alternatives A and B and prefer the 'none of these' option. Effects relating to these three statements only are used to capture the perception of usefulness and are found to be significant:

- A system that stores health information (such as blood group, allergies and health conditions) can be useful in providing higher-quality treatments.
- A system that stores health-related information (such as blood group, allergies and health conditions) can be useful in preventing health epidemics (e.g. H1N1/swine flu).
- I am concerned that in a health emergency there could be an unacceptable delay due to the time spent in identifying the person needing help and their health conditions before the treatment.

3.2 Factors influencing the attitudes

As summarised in Section 3.1, attitudes can have a significant impact on respondents' preferences relating to security, surveillance and privacy. In this section we investigate the statements used to capture these attitudes in order to understand the socio-economic factors behind them.

In PACT D4.1, a set of indices were computed using Westin's methodology[28] from responses to a series of statements (manifest variables). The indices provide a means to capture the unobserved attitudinal factors relating to trust, privacy and security. They were used to understand respondents' relative standing on various issues and establish an evidence base on how different factors are perceived across the EU27. Specifically, the following sets of indices were calculated based on responses to questions from the survey:

1. Distrust Index.
2. Institutional Trust Index.
3. Privacy-related indices that capture respondents' concern for privacy in each of the three contexts.

The indices, though helpful for cross-country comparisons, do not provide enough information to understand the latent attitudinal constructs – general distrust, trust and privacy concerns. Furthermore, the indices are computed using equal weights for each of the underlying manifest variables. This assumption of equal weights is restrictive and simplistic. Therefore, to better understand the relative importance of the underlying manifest variables and the interrelation between different latent constructs we undertook additional analysis using structural equation modelling (SEM).[29] SEM combines factor analysis and other regression techniques and is used in a confirmatory sense to test the hypothesised associations. The findings from SEM provide an understanding of:

1. The relative importance of the latent attitudinal constructs (distrust, trust, risk taking, privacy concern) in explaining the manifest variables.
2. The socio-economic factors that influence the attitudes. This relationship is particularly useful in understanding the potential impact of a given security or privacy measure on a given population based on directly observed demographic and socio-economic characteristics such as age, gender, and income.
3. The interrelation between the attitudinal constructs (e.g. between distrust and privacy concern).

A number of different specifications of SEM model exist in the literature, and we have used Multiple Indicators Multiple Causes models (MIMIC)[30] to specify the relationship between the latent attitudinal constructs, manifest variables and socio-economic variables. In MIMIC models, the observed socio-economic variables affect the manifest variables through the latent constructs only (see Figure 33).

The interrelationship between different variables can be further defined in terms of two sub-models, the Measurement model and the Structural model. The Measurement model captures, through factor loadings, the relationship between the manifest variables and the underlying latent constructs. The magnitude of the factor loadings determines the relative importance of the latent construct for each of the manifest variables. The Structural model captures the relationship between the latent constructs and the observed (socio-economic) variables.

[28] Kumaraguru, Ponnurangam, and Lorrie Faith Cranor, *Privacy Indexes: A Survey of Westin's Studies*, Institute for Software Research International, Carnegie Mellon University, Pittsburgh PA, 2005.
[29] Anderson, James C., and David W. Gerbing, "Structural Equation modelling in Practice: A Review and Recommended Two-Step Approach", *Psychological Bulletin*, Vol. 103(3), 1988, pp. 411–423.
[30] See http://www.stata.com/manuals13/semexample10.pdf

In the following sub-sections, we summarise the findings from the SEM models in each of the three SP contexts. To aid the understanding of the model a path diagram is included that shows the relationship between the three different types of variables.

3.2.1 Travel

The statements used in the Travel context choice model (Appendix B, Tables B.1, B.2) can be hypothesised to capture a concern for privacy, distrust and surveillance (see Figure 33). These hypotheses are tested using a structural equation model. Furthermore, the role of different socio-economic and context-specific variables as the determinants of these attitudes is also investigated.

The path diagram in Figure 33 shows the relationship between the three different types of variables specified in the Travel context. The rectangular boxes shaded in green represent the manifest variables, the oval shaped boxes shaded in pink represent the latent attitudinal constructs and rectangular boxes shaded in orange represent the socio-economic factors that influence the attitudes. The relationship between each of the variables is indicated by arrows: the blue one-headed arrows represent a linear relationship between the variables; the two-headed black arrows represent a correlation between the latent attitudinal variables. In addition, the factor loadings relating to each manifest variable are displayed on the top of the corresponding arrows, and the regression coefficients are displayed on top of the arrows connecting socio-economic variables. Higher values of factor loadings imply that the manifest variables are good indicators of the latent constructs and vice versa. For example a person with a higher concern for privacy is more likely to exhibit high concern for the misuse of CCTV camera images by the authorities. The regression coefficients can be interpreted in the usual way.

The relationship between the latent variables, the manifest variables and the socio-economic variables is discussed below. The full set of results, which includes the standard error and t-ratio of all the estimated parameters, is presented in Appendix C (Table C.1).

The results of the SEM imply that the statements used in the choice model are successful in capturing attitudes relating to general distrust and Travel context-specific privacy and surveillance concerns. The only exception is for the statement capturing (dis)trust in business, which is not necessarily a good measure of how generally distrustful an individual is.

A series of respondents' demographic features and travel characteristics are tested, including age, gender, monthly household income, education level, employment status and travel frequency and journey length. Below are the socio-economic and Travel context-specific variables that influence attitudes and are significantly estimated (at the 95 per cent confidence level) from the model:

- Age – Older respondents are more likely to be distrustful but are less likely to be concerned about privacy.
- Income – Respondents with higher income are less likely to be distrustful, concerned about privacy, or have strong concerns about surveillance.
- Gender – Men are less likely to be distrustful but are more likely to have strong concerns about surveillance.
- Travel frequency – Respondents who travel frequently are less likely to be distrustful. This variable is not significant in regressions with latent constructs of privacy and surveillance concerns.

The SEM specified in Figure 33 also tests for the association between latent variables. We find positive association between all three latent constructs. Particularly, we find that respondents who are more

distrustful are also likely to have greater surveillance concerns. Furthermore, respondents who have a high concern for privacy are also likely to have a high concern for surveillance.

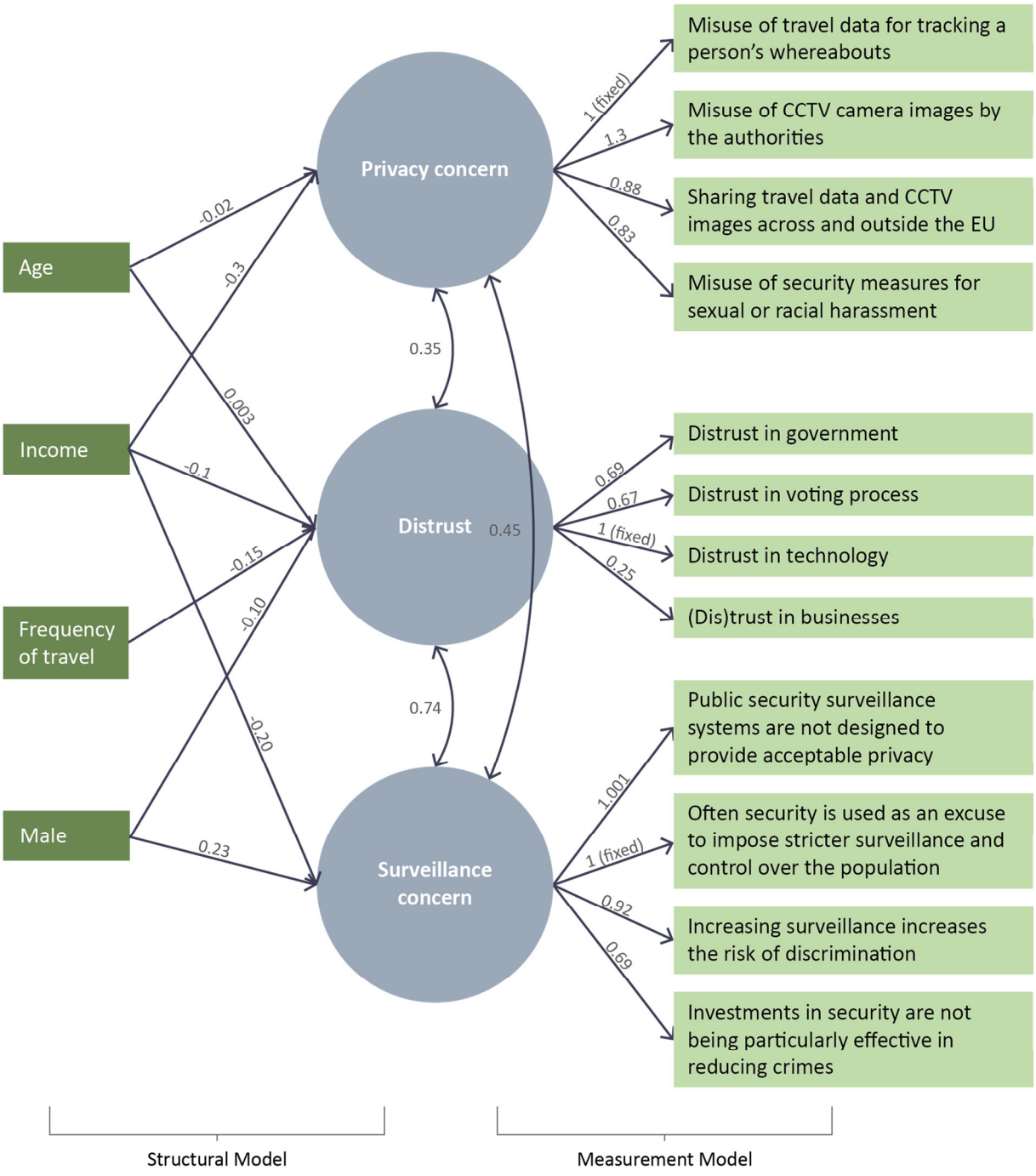


Figure 33: Determinants of attitudes in the Travel context

3.2.2 Internet

Similarly to the Travel context, the statements used in the Internet context are hypothesised to capture the Internet context privacy concern, security concerns relating to the use of Internet and general distrust. These hypotheses are summarised in Figure 34.

The path diagram in Figure 34 shows the SEM specification used in the Internet context. The effect of latent variables on the manifest variables and the effect of socio-economic determinants on each latent variable are discussed below. The full set of results is presented in Appendix C (Table C.2).

The results of the SEM imply that in general the statements used in the Internet context choice model are successful in capturing attitudes relating to Internet context privacy concern, security concerns relating to the use of Internet and general distrust. Two statements, however, do not necessarily measure the hypothesised latent construct of Internet security concern well (factor loading of 0.15 or less). The remaining three statements are closely associated with the latent construct and it could be argued that this latent construct captures distrust in websites rather than security concerns relating to Internet usage. Accordingly we observe a positive association (0.49) between this latent construct (distrust in websites) and general distrust. The association between the latent variables of Internet privacy concern and general distrust is positive (0.18), though not as high as in the Travel context.

We observe the following statistically significant socio-economic and Internet context-specific determinants of the attitudes:

- Age – Similar to the finding in the Travel context, older respondents are less likely to have concerns about privacy.
- Income – Respondents with higher income are more likely to be distrustful in general and they have fewer concerns about Internet privacy.
- Working status – People in full-time or part-time work are less likely to have security concerns regarding Internet usage.
- Education – Respondents who have tertiary education or higher are more concerned about Internet privacy and are more likely to have security concerns regarding Internet usage.
- Time spent on the Internet – Respondents who spend more than 20 hours a week browsing the Internet are less likely to be concerned about Internet usage security, but they are more likely to be distrustful in general and have strong Internet privacy concerns.

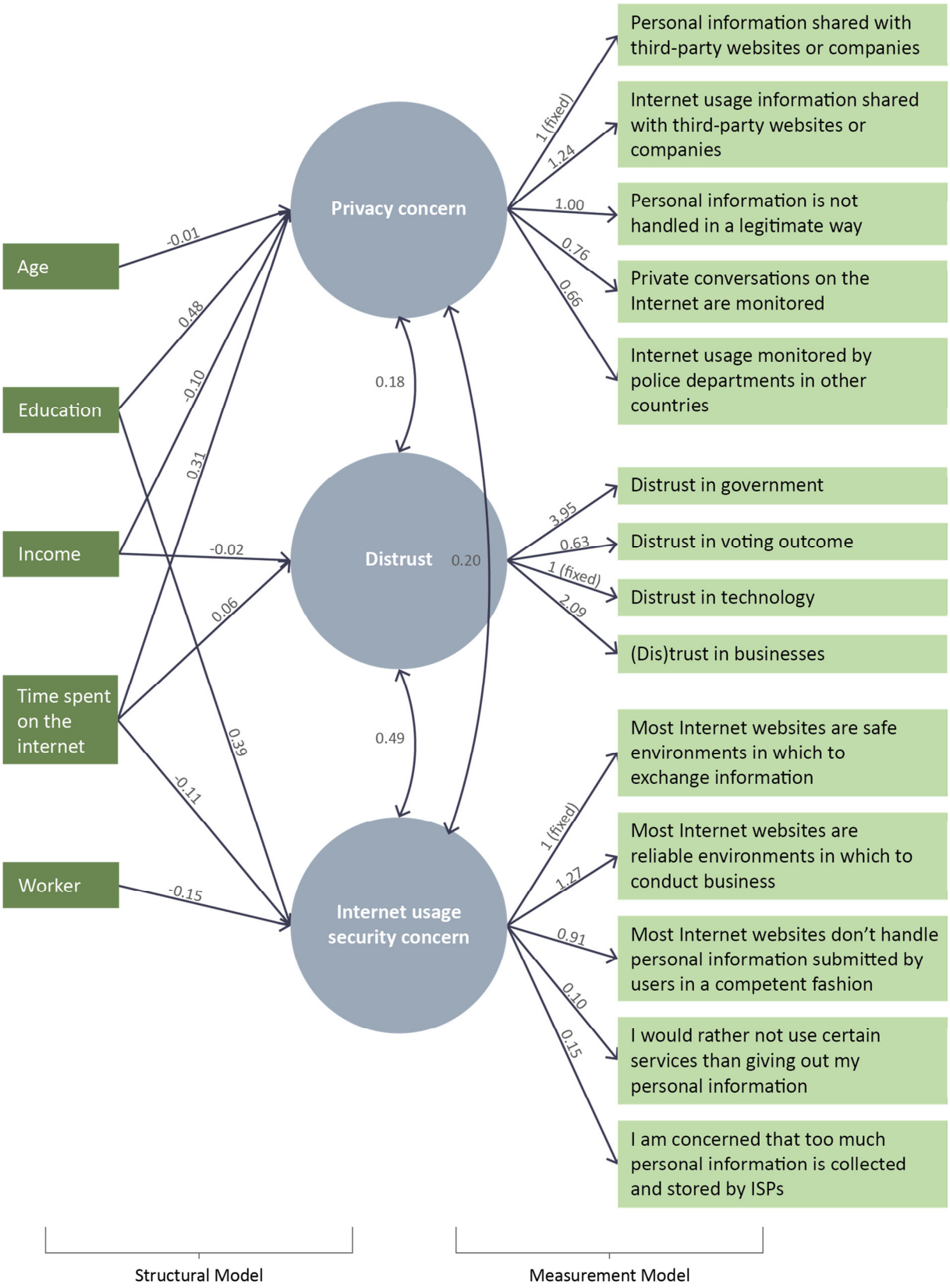


Figure 34: Determinants of attitudes in the Internet context

3.2.3 Health

As for the previous two contexts, the path diagram in Figure 35 shows the relationship between the different variables specified in the Health context. In this context a total of three latent variables are included: respondents' concern for privacy in the Health context, general distrust and respondents' general attitude towards the usefulness of health data storage devices/systems. The effect of latent variables on the manifest variables and the effect of the socio-economic determinants on each latent variable are discussed below. The full set of results is presented in Appendix C (Table C.3).

The results of the SEM imply that the statements used in the Health context choice model are successful in capturing attitudes relating to general distrust and Health context-specific privacy and attitudes towards the usefulness of such a device/system.

We observe the following socio-economic and Health context-specific factors that influence the attitudes:

- Age – Older respondents are less likely to be distrustful but are more likely to believe in the usefulness of a health data storage device/system.
- Income – Respondents with higher income are less likely to be distrustful or concerned about privacy, and are less likely to believe in the usefulness of a health data storage devices/system.
- Gender – Men are less likely to have privacy concerns or to believe in the usefulness of a health data storage device/system.
- Education – Respondents who have tertiary education or higher are more concerned about privacy and are less likely to believe in the usefulness of a health data storage device/system.
- Current health conditions – compared to respondents who do not require long-term treatment, those who do require long-term treatment have higher privacy concerns but are less distrustful.

The SEM specified in Figure 35 also tests for the association between latent variables. We find a positive association between privacy concern and general distrust (0.13), although the magnitude is smaller than that in the Travel context (0.35). We also find that respondents who are more distrustful are less likely to believe in the usefulness of a health data storage device/system (a correlation of -0.24).

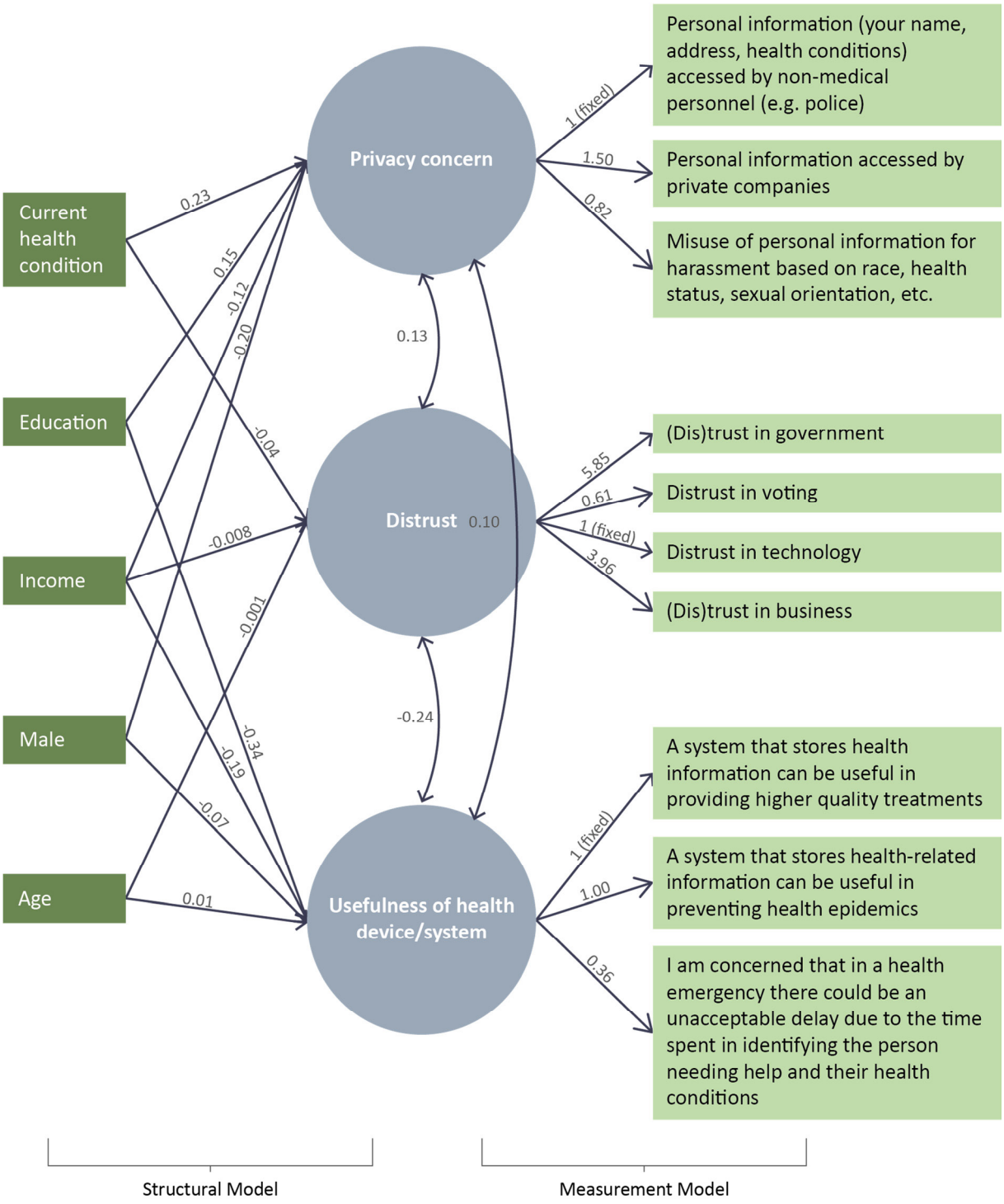


Figure 35: Determinants of attitudes in the Health context

3.3 Summary

This chapter has presented a summary of the analysis conducted to understand the effect of attitudes on preferences towards security, surveillance and privacy. The analysis was split into two stages. The first consisted of adding the manifest variables that are derived from the statements designed to capture the attitudes in the choice models. In the second stage the socio-economic and context specific variables that have an impact on the observed manifest variables through the underlying latent attitudinal constructs were investigated.

We find that respondents' attitudes as captured through the manifest variables significantly affect their preferences relating to security, surveillance and privacy. In general, the results of including attitudinal variables in the discrete choice models indicate that the greater the general distrust and the greater the concern for privacy in a given context, the more likely a respondent is to choose the 'none of these' alternative. The combination of attributes on offer does not, therefore, satisfy their concerns for privacy and security. The concern for privacy and the level of distrust are also reflected in the preferences for different security and privacy attributes, so that, for example, a respondent with concerns about privacy is less likely to want data stored on the Internet, although we did see some counter-intuitive results.

From the structural equation modelling, it is found that, for all three contexts, attitudes are influenced by age, gender and income. While education is a factor for attitudes relating to the Internet and Health, we do not identify a significant relationship in attitudes relating to Travel. Moreover, context-specific factors are also observed: travel frequency; time spent on the Internet; and current health condition. These arise from the investigation of separate attitudes to privacy concerns in each context as well as general distrust.

4. Conclusions and policy recommendations

PACT is a three-year pan-European project. The empirical work undertaken in Work Package 2 involved designing a survey instrument to measure public perceptions relating to security and privacy. Data collection across the EU27 was carried out using both online and face-to-face surveys as part of Work Package 3. The contexts explored in the PACT questionnaire include:

1. Travel on metro or train (Travel)
2. Choice of an Internet service provider (Internet)
3. Choice to purchase a device or service for storing health information (Health).

The stated preference scenarios used in these contexts describe choices between different hypothetical alternatives. Each alternative is described using attributes such as type of security and surveillance measures and issues relating to data handling in a scenario. In Work Package 4, respondents' choices across these scenarios are analysed to understand and quantify their preferences relating to security and privacy. Some preliminary analysis of these preferences was undertaken in Task 4.1. This analysis has been extended in Task 4.2 to include country-specific and socio-economic effects and to develop a quantitative framework for assessing the impact of attitudes on preferences.

Thus the main aim of Task 4.2 is to provide an understanding of preferences for privacy, security and surveillance for the three contexts of Travel, Internet and Health across the EU27 and how these differ between countries and socio-economic groups. In D2.4, hypotheses were developed through a rigorous literature review (WP1) to provide a framework for understanding these preferences, and these formed the basis for the survey questionnaires. The outcomes of the stated preference survey and consequent choice modelling exercise are therefore most sensibly presented in terms of these hypotheses. A similar exercise was carried out in Task 4.1 for the preliminary model results, without any country-specific or socio-economic effects. In this chapter we present preferences in terms of acceptance or rejection of the hypotheses for the full model and discuss how they have been influenced by these additional effects.

It should be noted that the discrete choice models used in Task 4.2 can be further extended to account for multiple responses from individuals (panel effect). However, due to the very large size of the dataset in each context, the panel version of such models takes multiple days for estimation. Hence we do not explicitly account for correlation between multiple responses from each respondent in the model. However, we use a bootstrap resampling approach, as a final step of the model estimation, to minimize the influence of the repeated nature of the SP data in the estimation of standard errors for the WTP estimates.

Furthermore, even though the choice models include country-specific effects where they are significantly different from average values, we do not estimate separate models for each of the EU27 countries. The country-specific models are out of the scope for this study, which focuses on Europe-wide aggregated evidence. Moreover, we observe surprising levels of consistency in values across the EU27 countries.

As part of the analysis we estimate willingness to pay (and willingness to accept) for different security and privacy measures. We emphasise that the WTP/WTA estimates derived from stated preference studies are often overestimates of actual values and can be influenced by the survey design. Therefore, the values should be used with some caution when quantifying the proposed benefits. However, this study provides possibly the first evidence of pan-European willingness to pay for security, surveillance and privacy measures/settings in the three contexts under consideration.

It should also be noted that there are multiple ways in which attitudes can be analysed. The reduced form discrete choice models used in this study incorporate attitudes in a simple way. It is possible to extend the models to simultaneously estimate the preferences and determinants of attitudes in one model using integrated choice and latent variable models. Such models, however, take substantial resources and were not feasible within the timescales and budget of this work package.

Below we summarise the findings from the discrete choice models developed in Task 4.2 using PACT's hypotheses. Given the complex nature of the attitudinal analysis, attitudes are not included in the discussion of the hypotheses below. Instead, the impact of attitudes on preferences is discussed separately. The implications of all the analysis are then drawn together in some final comments.

4.1 Travel

In the Travel context, preferences for privacy, surveillance and security were assessed in terms of their specific preferences relating to the presence of CCTV cameras, security personnel and physical security checks. The results of the hypothesis testing are summarised in Table 2.

In addition, in Figure 36 we summarise the countries that stand out among the EU27 in terms of their preferences relating to some of the attribute levels in the Travel context.

Table 2: Research hypotheses testing in the Travel context

Number	Research hypotheses	Findings
H1.1	Respondents prefer having CCTV cameras when travelling by metro/train.	Accept: all countries
H1.2	When CCTV is present, respondents prefer cameras with additional capabilities (e.g. abandoned bag detection and face recognition).	Reject: Sweden Accept: all other countries
H1.3	When CCTV is present, respondents prefer settings with CCTV footage only used in real time versus those in which the footage is stored for a specific number of days (3, 7, 15, 45 days).	Accept: Greece Reject: all other countries
H1.4	When CCTV is present, respondents prefer settings in which only the police departments in their country have access to CCTV footage compared to those in which European or worldwide police departments can access the CCTV footage.	Accept: all countries
H1.5	Respondents prefer having security personnel at the stations.	Reject: Germany, Hungary, Czech Republic, Poland, UK Accept: all other countries
H1.6	Respondents prefer police compared to private security forces.	Accept: Unarmed Police, all countries Armed police (Belgium, Germany, France, Ireland, and the U.K.) Reject: Armed policy (all others)
H1.7	Respondents prefer unarmed personnel (police or private) over armed personnel.	Police: Reject: Belgium, France Accept: all other Private: Reject: Greece, Accept: all other
H1.8	Respondents prefer travel options with no physical security checks (pat-down, bag search, metal detector and full body scanner).	Reject: Bulgaria, UK, France, Italy, Spain Accept: all other countries
H1.9	Respondents prefer options with metal detectors or full body scanners compared to those involving pat-downs and bag checks.	Reject: Luxembourg Accept: all other countries
H1.10	Respondents prefer travel options that involve no delay due to physical security checks.	Accept: all
H1.11	Respondents prefer travel options that involve no additional cost relating to security and surveillance measures.	Reject: WTP for some security/surveillance measures

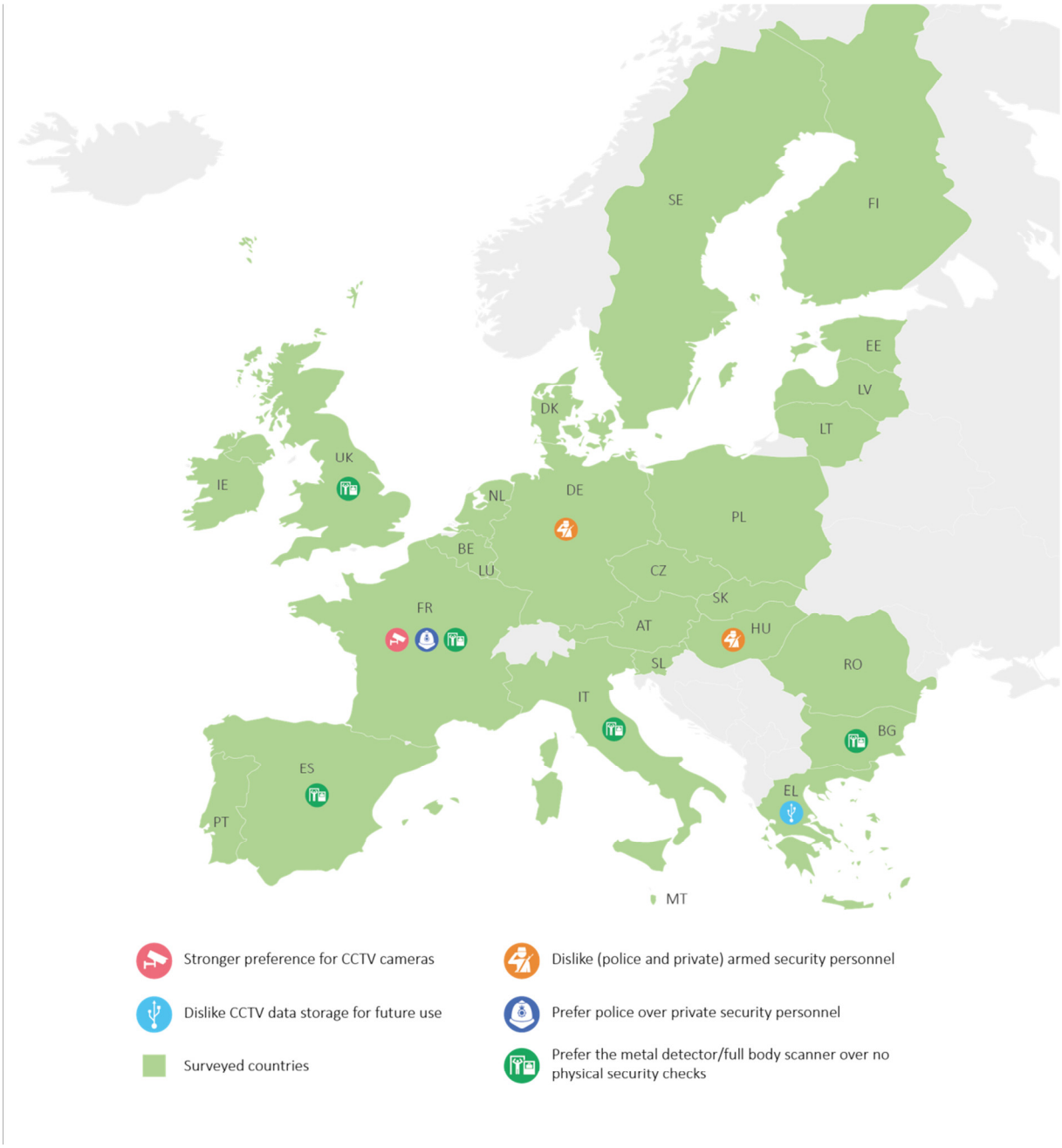


Figure 36: Countries with outlying preferences in the Travel context

4.2 Internet

The hypotheses relating to the Internet context cover preferences for data storage, access, surveillance and services to improve online protection. The results of testing these hypotheses are presented in Table 3.

Table 3: Research hypotheses testing in the Internet context

Number	Hypotheses	Findings
H2.1	Respondents prefer Internet Service Providers (ISPs) that do not collect Internet usage data over those who do.	Reject: Bulgaria, Latvia, Lithuania Accept: all other countries
H2.2	Respondents prefer ISPs that store less Internet usage data compared to those that store more information.	Accept: all countries
H2.3	Respondents prefer ISPs that do not provide access to Internet usage information to any law enforcement authorities.	Accept: all countries
H2.4	Respondents prefer ISPs that provide access to authorities only in their country of residence compared to those ISPs that can provide access to European or worldwide authorities.	Accept: all countries
H2.5	Respondents prefer ISPs that store Internet usage data for shorter durations.	Reject: Latvia Accept: all countries
H2.6	Respondents prefer ISPs that never allow continuous surveillance of its Internet users by law enforcement authorities.	Reject: all countries
H2.7	Respondents prefer ISPs that allow continuous surveillance of its Internet users only with a warrant compared to those ISPs that allow surveillance any time without a warrant.	Accept: all countries
H2.8	Respondents prefer ISPs that offer services to improve respondent's online privacy.	Accept: all countries
H2.9	Respondents prefer ISPs that do not charge for Internet security and data management.	Reject: WTP for services to improve privacy

Figure 37 summarises the countries that stand out among the EU27 in terms of their preferences relating to some of the attribute levels in the Internet context.

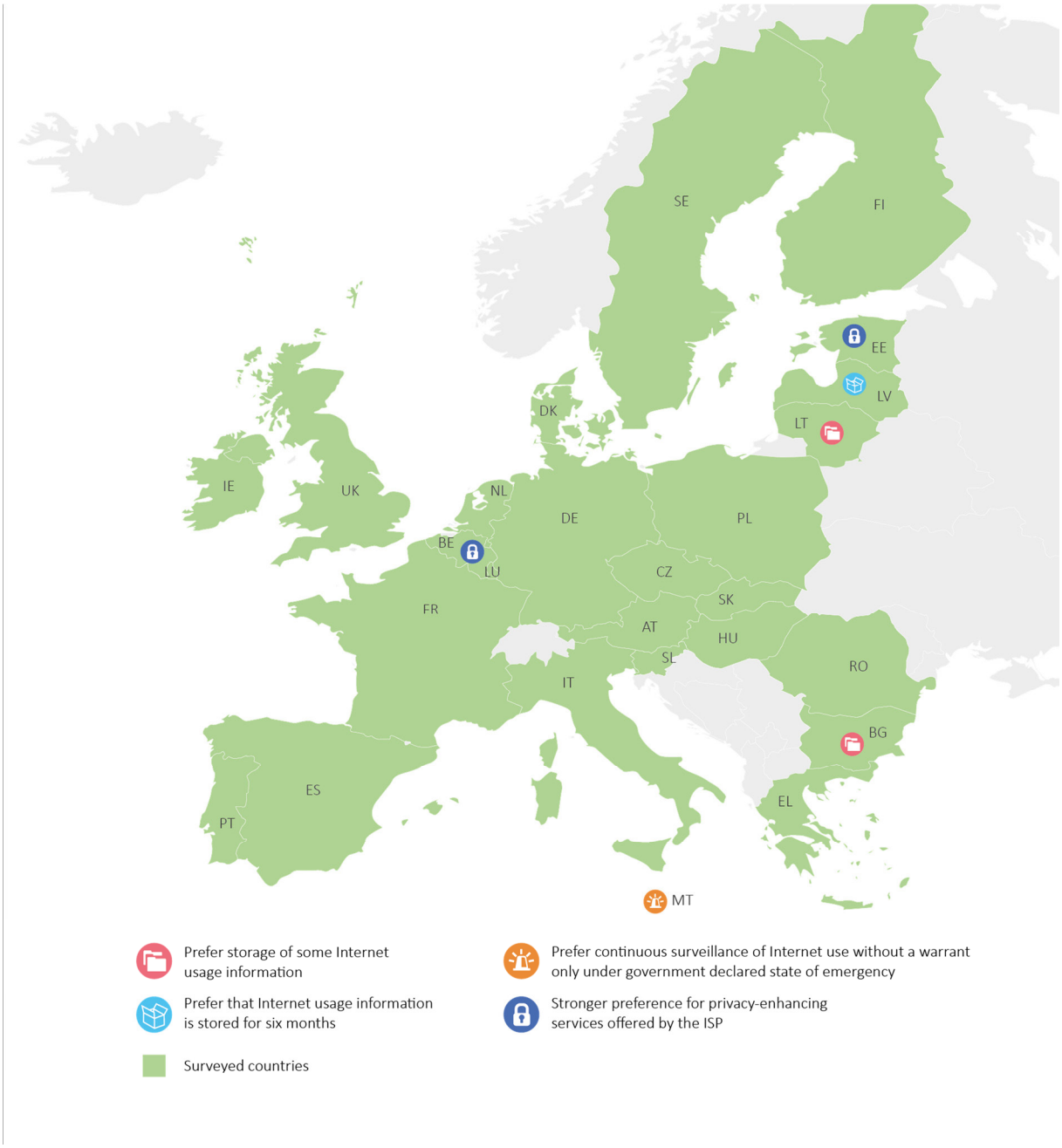


Figure 37: Countries with outlying preferences in the Internet context

4.3 Health

For the Health context, concerns for privacy, security and surveillance were elicited through hypotheses relating to respondents' preferences for health record devices/systems and the range and type of access to health data. The results for testing these hypotheses are summarised in Table 4.

Table 4: Research hypotheses testing in the Health context

Number	Hypotheses	Findings
H3.1	Respondents prefer a device/system with enhanced health or personal identification information compared to those with only basic health status information.	Reject: Czech Republic, Lithuania Accept : all other countries
H3.2a	Respondents prefer that only doctors and nurses have access to information compared to access also by paramedics	Accept: Slovenia Reject: others
H3.2b	Respondents prefer that only doctors and nurses have access to information compared to access also by paramedics, non-medical emergency personnel or any other state or private institutions.	Accept: all countries
H3.3	Respondents do not prefer device/service that can provide wider access outside their own country (EU/worldwide).	Accept: Austria, Czech Republic, Slovakia, age >65 Reject: all other countries
H3.4	Respondents do not prefer a health-records device/service to which health insurance providers, pharmaceutical companies and researcher could have access.	Accept: all countries
H3.5	Respondents prefer device/service that is free over a device/service that charges a fee per month.	Accept: at the device level Reject: WTP for some data and access options

Similarly to the other two contexts, the countries that stand out among the EU27 in terms of their preferences relating to some of the attribute levels in the Health context are presented in Figure 38.

Figure 38: Countries with outlying preferences in the Health context

4.4 The influence of attitudes on preferences

In order to understand the effect of attitudes on preferences we extend the choice models to include the attitudinal manifest variables. These are derived from statements to which respondents provide answers on a Likert scale. They measure the underlying latent attitudes relating to security, surveillance, privacy and distrust, albeit imperfectly.

We find that respondents' attitudes as captured through the manifest variables significantly affect their preferences relating to security, surveillance and privacy. In general, the results of including attitudinal variables in the discrete choice models indicate that the greater the level of general distrust and the greater the concern for privacy in a given context, the more likely a respondent is to choose the 'none of these' alternative. The combination of attributes on offer does not, therefore, satisfy their concerns for privacy and security. The concern for privacy and level of distrust are also reflected in the preferences for different

attribute levels, so that, for example, a respondent with concerns about privacy is less likely to want data stored on the Internet, although there are some counter-intuitive results.

In order to understand the factors that influence attitudes, we undertook structural equation modelling. The SEMs help us to understand the interrelations between attitudes and socio-economic variables. We find that for all three contexts, general distrust is influenced by income, with respondents indicating less distrust with increasing income. Furthermore, respondents with higher income are also less likely to have privacy concerns in all three contexts. Older respondents indicate more distrust in the Travel context but less distrust in the Health context. Older respondents are also less likely to be concerned about Travel and Internet privacy. While education influences attitudes in the Internet and Health contexts, it does not play a significant role in attitudes towards Travel. Moreover, context-specific factors are also observed to influence attitudes: travel frequency; time spent on the Internet; and current health condition. We also observe strong positive correlation between general distrust and surveillance concern in the Travel context.

4.5 Policy recommendations

PACT's data, analysed using stated preference methodology, provides the first evidence of its kind relating to issues of security, surveillance and privacy across Europe. The study aimed to understand the interrelationships between these issues using preferences provided by over 26,000 respondents across the EU27. The analysis conducted under WP4 (Tasks 4.1 and 4.2) offers many interesting findings relevant for policymaking involving issues of security and privacy:

- **Preferences depend on the context** – Preferences for security, surveillance and privacy depend on the context. Furthermore, in a given context the preferences are affected by other relevant characteristics such as extent of use (Travel, Internet) and circumstances (existing health conditions in the Health context). Thus the regulations/infrastructure designed around security and privacy need to address any context-specific issues.
- **Acceptability of surveillance and security measures depends on level of access to personal information** – Respondents prefer some security and surveillance measures but only under certain terms relating to geographic access and type of personnel involved in security and surveillance. Indeed, respondents prefer local access to surveillance/personal data covering country of residence or the EU in some cases. Respondents also indicate different preferences for types of personnel involved and indicate stronger preferences for accountability in terms of the requirement for a warrant to access personal data. These preferences, collected just after the revelation of secret surveillance programs by the NSA and GCHQ in 2013, add an important piece of evidence to the debate relating to privacy and data protection.
- **Privacy has multiple layers** – Comparison of findings across contexts points to different preferences relating to different layers of privacy. The data collection suggested in each of the three contexts gets increasingly personal and accordingly the preferences regarding terms of access to these data vary. While respondents are more willing to accept surveillance in the Travel context, they are averse to it in the Internet context.
- **Privacy-enhancing technologies are preferred** – Respondents indicate a strong preference for all types of assistance provided by Internet Service Providers to help protect the privacy of its users.
- **Preferences are not very different across Europe** – While the level of similarity of preferences observed across the EU27 is noteworthy, there are interesting differences. For example, in countries that have experienced terrorism on transport facilities in recent past, respondents indicate a preference for metal detectors in the Travel context, unlike other countries in EU27.

- **Respondents are willing to pay for security, surveillance and privacy measures** – In general respondents are averse to paying additional costs for security and surveillance. However, the experiments do provide evidence of WTP for some measures, with WTP varying depending on the context and attribute (security/surveillance/privacy feature/measure).
- **Certain groups of respondents have different preferences than others** – Some segments of society indicate different preferences compared to others. We find that respondent's age, gender, income, education and work status can affect their preferences. The security and surveillance infrastructure needs to take into account the needs of various segments of society. For example, it is found that women show stronger preferences for CCTV cameras in the Travel context compared to men; whilst younger people (aged 18 to 24) show stronger disinclinations towards physical security checks and the presence of CCTV cameras compared to the other age groups.
- **Attitudes can play a role in shaping preferences** – We find that attitudes play a significant role in shaping preferences relating to security and surveillance. Accordingly, steps taken to inform, educate and assure the public will be beneficial to relieve their concerns in each context.
- **Reject the trade-off model** – Syntheses of our findings (discussed in D4.1) indicate that respondents' preferences relating to security and privacy are much more nuanced than a simplistic inverse relationship implied by a trade-off model of security and privacy. This simplistic model – which is often articulated by policymakers and portrayed in the media – is frequently used to characterise additional security and surveillance measures as being at the cost of privacy and liberty.

Acknowledgements

The authors would like to express their gratitude to RAND Europe's Quality Assurance team, especially Ms. Charlene Rohr and Dr. Matthew Bassford for their useful comments on how to improve this report. We also wish to thank Prof. Andrew Daly (RAND Europe) for his guidance on the analysis. In addition we thank the PACT project consortium partners from ATOS and Demokritos for their comments on the report. However, any errors or omissions herein remain the responsibility of the authors.

Appendix A: Modelling the effects of country and socio-economic factors on preferences relating to security, surveillance and privacy

Model specification

Report D4.1 Appendix E provided a brief introduction to the random utility theory and discrete choice modelling framework used to estimate the responses to the stated preference exercises.

The overall utility of a choice alternative *i* for responses *n* is represented below:

$$U_{ni} = V_{ni} + \varepsilon_{ni}$$

where V_{ni} represents the deterministic or the measurable part of the utility and ε_{ni} is the error term that represents the unobserved component of the utility and is assumed to be independent and identically distributed (iid) over all the alternatives and respondents. It is assumed that respondents choose the alternative that maximises their utility. The distributional assumptions relating to ε_{ni} give rise to different types of models. In case of a multinomial logit model (MNL), the error term is assumed to follow a Type 1 extreme value distribution (Gumbel) and the resultant probabilities are:

$$V_n = \sum_k \beta_k * X_{njk}; P_{ni} = \frac{e^{V_{ni}}}{\sum_{j=1}^{J} e^{V_{nj}}}$$

where β_k is the vector of parameters of the k^{th} attributes (X_{nik}) and their levels. The product of probabilities across all responses is maximised (maximum likelihood method) to estimate the vector of parameters.

To incorporate the country-specific and socio-economic effects on preferences, segmentation analysis (Train, 2003)[31] is deployed in the models to account for the variation of the different respondent groups. To do this, an incremental factor is included:

$$\sum_{y=1}^{n-1} \gamma_{yk} * d_{yik} * x_{nik}$$

where γ_{yk} is an incremental factor for the k^{th} attribute (X_{nik}), and d_{yik} is a dummy variable denoting whether or not an observation is in y^{th} groups of *n* groups in a category (such as one of the EU27 countries). If so, d_{yik} is one, otherwise zero; one of the groups is selected as the base, and the incremental effects for other groups are relative to the base, so there are n-1 dummy variables defined.

In the present study, there are three alternatives: Alt A, Alt B and 'none of these'. Then the utility functions and resulting probabilities are shown:

V[Alt A] = $\sum_k \beta_k * X_{Ak} + \sum_{y=1}^{n-1} \gamma_{yk} * d_{yk} * x_{yAk}$; P[Alt A] = $e^{V[Alt\ A]}$/ ($e^{V[Alt\ A]} + e^{V[Alt\ B]} + e^{V[none]}$)

V[Alt B] = $\sum_k \beta_k * X_{Bk} + \sum_{y=1}^{n-1} \gamma_{yk} * d_{yk} * x_{yBk}$; P[Alt B] = $e^{V[Alt\ B]}$/ ($e^{V[Alt\ A]} + e^{V[Alt\ B]} + e^{V[none]}$)

[31] Train, Kenneth, *Discrete Choice Methods with Simulation*, Cambridge University Press, Cambridge, 2009.

V[none] = $\beta_{none} + \sum_{y=1}^{n-1} \gamma_y * d_y$; P[none] = $e^{V[none]}$/ ($e^{V[Alt\ A]}$ + $e^{V[Alt\ B]}$ + $e^{V[none]}$)

For Alt A and Alt B, the coefficient of attribute X_k for the base group is defined by β_k, and the coefficient of X_k for the y^{th} group respondents is $\beta_k + \gamma_{yk}$. For the 'none of these' alternative, the effect is $\beta_k + \gamma_y$ for the y^{th} group in the category. This approach can indicate the sign and magnitude of any effects from the segmentation variables, provided they are statistically significant.

Table A.1: Travel model results

Model file	Travel_v57.F12		
Estimation Date	30-Apr-14		
Estimation Time	15:53:02		
Summary statistics			
Observations	60472		
Final Log Likelihood	-61319.3		
D.O.F	137		
$Rho^2(0)$	0.077		
$Rho^2(c)$	0.054		
Description	**Label**	**Coefficient**	**t-ratio**
Type of CCTV cameras			
Standard CCTV – working like a television	cam_std	0.8358	12.64
Advanced CCTV that can detect abandoned bags	cam_bag	0.9429	13.15
Advanced CCTV that can recognise suspicious movements of people	cam_sus	0.8718	12.69
Advanced CCTV that can recognise faces	cam_face	0.9785	13.24
No CCTV cameras	cam_none	0	n/a
How long CCTV camera information is stored			
CCTV information not stored for future use – only real-time monitoring	dur_rt	0.0000	n/a
CCTV information stored for 3 days	dur_3d	0.1801	6.82
CCTV information stored for 7 days	dur_7d	0.3156	9.80
CCTV information stored for 15 days	dur_15d	0.3225	10.09
CCTV information stored for 45 days	dur_45d	0.1666	6.23
Who can access CCTV camera information			
Only police departments in the [UK] have access to the camera information	acc_op	0.0000	n/a
All European police departments have access to the camera information	acc_eu	-0.1261	-6.83
All police departments worldwide have access to the camera information	acc_int	-0.2327	-9.72
Security personnel at the station			
No security personnel	per_none	0	n/a
Unarmed security personnel employed by a private company	pers_pvt	0.3115	10.24
Armed security personnel employed by a private company	pers_ta	0.2336	8.32
Unarmed police	pers_pol	0.4450	11.78
Armed police	pers_arm	0.2205	7.83
Type of security checks at the station			
People randomly selected for physical search and bag check	sec_pd	-0.2449	-9.50
People randomly selected to go through metal detector or full body scanner	sec_md	-0.0318	-1.65
No physical security checks	sec_none	0	n/a
Time to go through security checks			
10 seconds 30 seconds 1 minute 2 minutes 5 minutes	time	-0.0003	-8.55
Security surcharge on top of ticket cost			
HH Income less than €500	cost_1t4	-0.0074	-10.05
HH Income from €500 to €1,250	cost_5t6	-0.0059	-10.28
HH Income from €1,250 to €5,000	cost_7t14	-0.0040	-11.40
HH Income greater than €5,000	cost_gt14	-0.0033	-5.17
Missing Income (Low-income countries)	cost_NA_L	-0.0134	-10.16
Missing Income (Medium-income countries)	cost_NA_M	-0.0066	-7.02
Missing Income (High-income counties)	cost_NA_H	-0.0071	-3.11

Description	Label	Description	Coefficients	t-ratio
Type of CCTV cameras				
Standard CCTV – working like a television	cam_std_SE	Sweden	0.2534	3.76
Advanced CCTV that can recognise faces	Camface_HU	Hungary	-0.2254	-3.39
No CCTV cameras	Nocam_BG	Bulgaria	0.5875	6.12
	Nocam_CZ	Czech Republic	0.7531	9.31
	Nocam_EL	Greece	0.6566	7.69
	Nocam_FR	France	-0.3605	-1.86
	Nocam_HU	Hungary	0.5636	7.07
	Nocam_LV	Latvia	0.5504	4.92
	Nocam_MT	Malta	0.0000	n/a
	Nocam_PL	Poland	0.4607	4.24
	Nocam_PT	Portugal	0.7008	6.45
	Nocam_SK	Slovakia	0.6238	6.44
	Nocam_male	Male	0.1715	5.20
	Nocam_1824	Age group 18–24	0.0954	1.91
	Nocam_5564	Age group 55–64	-0.1268	-2.98
How long CCTV camera information is stored				
CCTV information not stored for future use – only real-time monitoring	dur_rt_AT	Austria	0.1858	2.27
	dur_rt_EL	Greece	0.3542	4.65
	dur_rt_EE	Estonia	-0.3248	-3.68
	dur_rt_IE	Ireland	-0.2105	-2.84
CCTV information stored for 45 days	dur_45d_MT	Malta	0.0000	n/a
	dur_45d_ES	Spain	0.2400	3.33
	dur_45d_CZ	Czech Republic	-0.2153	-2.89
Who can access CCTV camera information				
acc_eu_LV	acc_eu_LV	Latvia	-0.2672	-2.78
acc_int_DE	acc_int_DE	Germany	-0.3473	-3.74
Security personnel at the station				
No security personnel	nospers_BE	Belgium	-0.2234	-2.87
	nospers_CY	Cyprus	-0.6167	-2.83
	nospers_CZ	Czech Republic	0.2399	3.94
	nospers_DE	Germany	0.2673	4.89
	nospers_ES	Spain	-0.4031	-4.99
	nospers_FR	France	-0.5466	-3.33
	nospers_HU	Hungary	0.2722	4.29
	nospers_IT	Italy	-0.2368	-2.66
Unarmed security personnel employed by a private company	perspvt_FR	France	-0.4115	-3.60
Armed security personnel employed by a private company	persta_DE	Germany	-0.4010	-5.58
	persta_EE	Estonia	0.1403	2.04
	persta_FR	France	-0.3465	-2.95
	persta_IE	Ireland	-0.2299	-3.60
	persta_UK	UK	-0.2682	-3.95
Armed police	persarm_BE	Belgium	0.2361	3.51
	persarm_FR	France	0.3735	3.67
	persarm_PL	Poland	-0.3400	-3.28
Type of security checks at the station				
No physical security checks	nosec_AT	Austria	0.2671	4.57
	nosec_CZ	Czech Republic	0.2064	3.62
	nosec_DE	Germany	0.4974	5.51
	nosec_DK	Denmark	0.1342	2.83
	nosec_ES	Spain	-0.1416	-2.88
	nosec_FR	France	-0.1850	-2.83
	nosec_IT	Italy	-0.2843	-4.26

	nosec_LV	Latvia	0.3802	4.23
	nosec_PL	Poland	0.3058	3.50
	nosec_SE	Sweden	0.2332	3.99
	nosec_SI	Slovenia	1.1783	2.76
	nosec_SK	Slovakia	0.2648	3.47
	nosec_UK	UK	-0.1284	-2.46
People randomly selected to go through metal detector or full body scanner	sec_md_BG	Bulgaria	0.1959	3.00
	sec_md_LU	Luxembourg	-0.2542	-3.50
	secmd_1824	Age group 18–24	0.0602	1.73

Country effects			
Country	**Label**	**Coef.**	**t-ratio**
Austria	Scale_AT	1.0000	n/a
Belgium	Scale_BE	1.1690	10.8
Bulgaria	Scale_BG	1.0387	6.6
Cyprus	Scale_CY	0.8774	5.3
Czech Republic	Scale_CZ	1.4830	6.7
Denmark	Scale_DK	1.5837	9.2
Estonia	Scale_EE	1.0703	10.7
Finland	Scale_FI	1.0903	11.0
France	Scale_FR	0.9150	6.7
Germany	Scale_DE	0.9054	8.9
Greece	Scale_EL	1.3550	6.6
Hungary	Scale_HU	1.6390	6.9
Ireland	Scale_IE	1.1664	11.3
Italy	Scale_IT	1.0825	9.6
Latvia	Scale_LV	1.0086	6.3
Lithuania	Scale_LT	0.6654	3.4
Luxembourg	Scale_LU	0.9271	9.5
Malta	Scale_MT	1.0878	6.3
Netherlands	Scale_NL	0.9444	9.9
Poland	Scale_PL	1.1924	6.4
Portugal	Scale_PT	1.0543	6.3
Romania	Scale_RO	0.6846	6.2
Slovakia	Scale_SK	1.1285	6.4
Slovenia	Scale_SI	0.4128	3.6
Spain	Scale_ES	1.2204	11.1
Sweden	Scale_SE	1.1708	11.0
UK	Scale_UK	1.1836	11.1
Survey method effects			
Online	Scale_O	1.0000	n/a
Face to Face	Scale_F	0.8298	10.3

None constant			
Country	**Label**	**Coef.**	**t-ratio**
Italy (Face)	None_IT_F	-0.0944	-0.7
Italy (Online)	None_IT_O	0.1007	1.0
UK	None_UK	0.2613	4.0
Sweden	None_SE	0.9846	11.5
Spain	None_ES	0.2735	4.0
Slovenia	None_SI	0.9659	4.4
Slovakia	None_SK	0.5923	7.2
Romania	None_RO	-0.4055	-2.5
Portugal	None_PT	0.5911	6.9
Poland	None_PL	0.8790	9.9
Netherlands	None_NL	0.3597	4.8
Malta	None_MT	-0.2613	-1.7
Luxembourg	None_LU	0.3513	4.2
Lithuania	None_LT	0.1498	0.6
Latvia	None_LV	-0.6409	-3.4
Ireland	None_IE	0.3804	6.0
Hungary	None_HU	1.0252	12.0
Greece	None_EL	0.3892	4.5
Germany (Face)	None_DE_F	0.4230	3.8
Germany (Online)	None_DE_O	0.7058	7.5
France	None_FR	-0.0833	-0.5
Finland	None_FI	0.7701	10.8
Estonia	None_EE	0.0811	1.0
Denmark	None_DK	1.1011	12.4
Czech Republic	None_CZ	0.9664	11.4
Cyprus	None_CY	0.2371	1.6
Bulgaria	None_BG	-0.6235	-3.7
Belgium	None_BE	0.5128	7.2
Austria	None_AT	0.7045	8.5

Table A.2: Internet model results

Model file	Internet_v48.f12		
Estimation Date	02-Apr-14		
Estimation Time	11:01:31		
Summary statistics			
Observations	74304		
Final Log Likelihood	-73439.7		
D.O.F	105		
$Rho^2(0)$	0.100		
$Rho^2(c)$	0.077		
Description	**Label**	**Coefficient**	**t-ratio**
Type of Internet usage information stored			
Websites you have visited	data_1	-0.3333	-7.7
Websites visited and your location	data_2	-0.4644	-11.4
Websites visited, your location, and list of persons you contact on the Internet	data_3	-0.7214	-16.3
All Internet activities including what you write in emails or type on websites	data_4	-0.8469	-19.4
No information will be stored	data_none		
How long Internet data are stored			
1 month	dur_1m	0.0000	n/a
6 months	dur_6m	-0.1223	-4.6
1 year	dur_1y	-0.2216	-7.7
5 years	dur_5y	-0.4664	-15.9
Who has access to Internet information			
Information will not be shared with anyone else	acc_none	0.0000	n/a
Information could only be shared with police departments in [UK]	acc_nla	-0.1439	-5.4
Information could be shared with all European police departments	acc_eu	-0.5101	-16.5
Information could be shared with police departments worldwide	acc_int	-0.6439	-20.2
When ISP can allow continuous surveillance of its Internet users by the police			
Any time without a warrant	cond_1	-1.0588	-30.2
Only with a warrant	cond_2	0.1525	5.4
Without a warrant but only under government declared state of emergency	cond_3	-0.3206	-11.3
Never	cond_4	0.0000	n/a
Services offered to improve online privacy			
ISP will not offer any service to improve your online privacy	serv_1	0.0000	n/a
ISP will advise on how to use Internet anonymously without allowing websites to collect your personal data	serv_2	0.7627	22.2
ISP will warn you which websites do not meet your desired level of privacy	serv_3	0.7792	22.3
ISP will actively hide information on your Internet use from others	serv_4	0.8186	21.2
Monthly cost or discount for Internet security and data management			
Discount (all income levels)	cost_d	-0.0011	-9.3
There is no impact on price (all income levels)	cost_n	0.3894	10.9
Cost if HH Income less than €500	cost_c1to4	-0.0028	-10.8
Cost if HH Income from €500 to €1,500	cost_c5to8	-0.0023	-14.1
Cost if HH Income greater than €1,500	cost_c921	-0.0015	-10.9
Discount (missing income)	cost_d_NA	0.0009	3.3
There is no impact on price (missing income)	cost_n_NA	-0.0598	-0.6
Cost (missing income) for low/medium-income countries	cost_NA_L	-0.0063	-15.6
Cost (missing income) for high-income countries	cost_NA_H	-0.0039	-7.8

Description	Label	Description	Coefficients	t-ratio
Type of Internet usage information stored				
No information will be stored	nodata_BG	Bulgaria	-0.6090	-4.2
	nodata_FI	Finland	0.2818	2.7
	nodata_LV	Latvia	-0.6816	-5.0
	nodata_LT	Lithuania	-0.8871	-5.4
Website you have visited	data_1_18		0.2818	4.5
All Internet activities	alldata_FI	Finland	-0.3530	-3.1
	alldata_IE	Ireland	-0.4063	-3.2
How long Internet data are stored				
1 year	dur_1y_LV	Latvia	0.3456	2.4
Who has access to Internet information				
Worldwide	acc_int_LU	Luxembourg	-0.2405	-2.6
	acc_int_SI	Slovenia	0.4946	4.0
When ISP can allow continuous surveillance of its Internet users by the police				
Any time without a warrant	cond_1_LT	Lithuania	-1.0610	-4.0
Only with a warrant	cond_2_DK	Denmark	0.3741	4.3
	cond_2_ES	Spain	0.5313	5.2
Without a warrant but only under government declared state of emergency	cond_3_LT	Lithuania	-0.8997	-4.7
	cond_3_55	Age 55–64	-0.1215	-2.6
Never	cond_4_65	Age over 65	-0.1217	-2.6
	cond_4_MT	Malta	-0.8110	-3.5
Services offered to improve online privacy				
ISP will not offer any service to improve your online privacy	serv_1_SK	Slovakia	0.3622	3.4
	serv_1_EE	Estonia	-0.2707	-3.6
	serv_1_CZ	Czech Republic	0.6194	5.7
	serv_1_BE	Belgium	-0.3052	-3.4
	serv_1_65	Age over 65	-0.1997	-3.8
	serv_1_man	Male	0.2495	6.8
None of these options				
	none_18	Age 18–24	-0.3918	-10.5
	none_25	Age 25–34	-0.1525	-5.4

Country effects			
Country	**Label**	**Coef.**	**t-ratio**
Austria	Scale_AT	1.0000	n/a
Belgium	Scale_BE	0.8529	20.9
Bulgaria	Scale_BG	0.6929	10.3
Cyprus	Scale_CY	0.4835	8.4
Czech Republic	Scale_CZ	0.7403	11.6
Denmark	Scale_DK	0.8555	19.1
Estonia	Scale_EE	1.0000	n/a
Finland	Scale_FI	0.8708	17.0
France	Scale_FR	0.8948	21.1
Germany	Scale_DE	1.0000	n/a
Greece	Scale_EL	0.5378	9.9
Hungary	Scale_HU	0.6845	11.2
Ireland	Scale_IE	0.7579	17.9
Italy	Scale_IT	0.7185	15.8

None constant			
Country	**Label**	**Coef.**	**t-ratio**
Italy (Face)	None_IT_F	-0.2072	-1.8
Italy (Online)	None_IT_O	0.0996	1.1
UK	None_UK	-0.0491	-0.8
Sweden	None_SE	0.4642	6.6
Spain	None_ES	0.2140	2.7
Slovenia	None_SI	0.1664	1.7
Slovakia	None_SK	0.0086	0.1
Romania	None_RO	-1.2532	-7.3
Portugal	None_PT	0.5987	4.0
Poland	None_PL	0.4478	3.5
Netherlands	None_NL	-0.0573	-1.0
Malta	None_MT	-2.2940	-8.5
Luxembourg	None_LU	0.1900	3.0
Lithuania	None_LT	-2.2461	-10.1

Latvia	Scale_LV	0.6891	11.0
Lithuania	Scale_LT	0.4964	8.5
Luxembourg	Scale_LU	1.0000	n/a
Malta	Scale_MT	0.4294	7.8
Netherlands	Scale_NL	1.0000	n/a
Poland	Scale_PL	0.5227	10.2
Portugal	Scale_PT	0.5280	9.3
Romania	Scale_RO	0.4342	8.4
Slovakia	Scale_SK	0.7644	11.9
Slovenia	Scale_SI	0.6335	11.1
Spain	Scale_ES	0.7229	17.8
Sweden	Scale_SE	0.9083	20.1
UK	Scale_UK	0.9105	21.1
Survey method effects			
Online	Scale_O	1.0000	n/a
Face to Face	Scale_F	0.8156	15.7

Latvia	None_LV	-3.2840	-14.9
Ireland	None_IE	0.0049	0.1
Hungary	None_HU	0.4510	4.3
Greece	None_EL	-0.9874	-7.9
Germany (Face)	None_DE_F	0.5174	5.4
Germany (Online)	None_DE_O	0.3430	4.9
France	None_FR	0.2986	4.5
Finland	None_FI	0.2286	2.8
Estonia	None_EE	-0.1328	-2.1
Denmark	None_DK	0.3460	4.5
Czech Republic	None_CZ	0.0479	0.5
Cyprus	None_CY	0.3209	2.2
Bulgaria	None_BG	-1.4896	-12.0
Belgium	None_BE	-0.1171	-1.8
Austria	None_AT	0.2120	3.5

Table A.3: Health model results

Model file	Health_v31.F12		
Estimation Date	28-Feb-14		
Estimation Time	15:34:24		
Summary statistics			
Observations	94606		
Final Log Likelihood	-93598.6		
D.O.F	117		
$Rho^2(0)$	0.099		
$Rho^2(c)$	0.079		
Description	**Label**	**Coefficient**	**t-ratio**
What information is stored on the device/system			
Basic health status	data_1	0.0000	n/a
Basic health status + Identification	data_2	0.0404	2.15
Basic health status + Identification + Lifelong health conditions	data_3	0.1300	5.30
Basic health status + Identification + Lifelong health conditions + All other health conditions and medical history	data_4	-0.0323	-1.18
Who can access the information			
Only doctors and nurses	acc_1	0.0000	n/a
Doctors, nurses, and paramedics	acc_2	0.0660	4.38
Doctors, nurses, paramedics and fire and rescue	acc_3	-0.0629	-2.43
In which countries your information can be accessed?			
Only in the home country	acch_ter	0.0000	n/a
Across Europe (EU)	acch_eu	0.0608	3.24
Worldwide	acch_int	-0.1415	-5.53
Who else can view this information apart from medical specialists?			
No one	view_non	0.0000	n/a
Immediate family	view_fam	-0.0534	-2.60
Nurses providing home care	view_nur	-0.0642	-2.96
Health insurance companies	view_ins	-0.4280	-9.11
Private sector pharmaceutical companies	view_pri	-0.8165	-9.28
Academic researchers	view_med	-0.5321	-7.90
Cost			
HH income less than €500	cost1t4	-0.0042	-10.05
HH income from €500 to €1500	cost5t8	-0.0036	-10.48
HH income from €1500 to €3000	cost9t11	-0.0031	-10.18
HH income from €3000 to €9000	cost12t18	-0.0028	-10.13
HH income greater than €9000	cost19t21	-0.0016	-2.35
Missing income	costNA	-0.0044	-9.29

What information is stored on the device/system	**Effects**	**Label**	**Coefficient**	**t-ratio**
Basic health status	Czech Republic	data_1CZ	0.1919	3.0
	Lithuania	data_1LT	0.2539	3.4
	UK	data_1UK	-0.1107	-2.0
	Age 18–24	data_1ag24	0.2783	4.6
Basic + Identification	Age 18–24	data_2ag24	0.2249	3.7
Basic + Identification + Lifelong health conditions	Age 18–24	data_3ag24	0.2897	4.3
	Age 25–34	data_3ag34	0.0980	2.5
	Age 55–64	data_3ag64	-0.0862	-2.3
Basic + Identification + Lifelong health conditions + All other health conditions and medical history	Cyprus	data_4CY	0.7192	3.3
	Male	data_4male	0.0570	2.0

	Age 18–24	data_4ag24	0.4157	5.6
	Age 25–34	data_4ag34	0.1782	4.4
Who can access the information				
Only doctors and nurses	Slovenia	acc_1SI	0.2974	3.6
Doctors, nurses, and paramedics	Estonia	acc_2EE	0.2351	3.3
Doctors, nurses, paramedics and fire and rescue	Denmark	acc_3DK	-0.1127	-2.1
	Age >= 65	acc_3ag65	-0.1094	-3.4
In which countries your information can be accessed?				
Only in the home country	Czech Republic	acch_tCZ	0.1808	2.9
	Slovakia	acch_tSK	0.1147	2.2
	Belgium	acch_tBE	-0.2480	-4.6
	Ireland	acch_tIE	-0.1909	-2.7
	Romania	acch_tRO	-0.3403	-4.6
	Spain	acch_tES	-0.2464	-4.1
	Age >= 65	acch_tgt65	0.1315	3.8
Across Europe (EU)	Austria	acch_eAT	-0.2089	-3.7
Worldwide	Slovakia	acch_iSK	-0.1035	-1.8
	Age 18 - 24	acch_i1824	0.1131	3.1
	Age 25 - 34	acch_i2534	0.1349	3.9
	Age >= 65	acch_igt65	-0.0977	-2.6
Who else can view this information apart from the medical specialists?				
No one	Austria	view_nAT	0.2105	2.7
	Luxembourg	view_nLU	0.2060	2.8
	Netherlands	view_nNL	0.2680	3.2
	Lithuania	view_nLT	-0.4326	-4.5
	Romania	view_nRO	-0.3884	-3.0
	Slovakia	view_nSK	-0.1925	-2.8
Immediate family	Slovenia	view_fSI	0.5197	3.5
Nurses providing home care	Belgium	view_nurBE	0.1650	2.0
	France	view_nurFR	0.2056	2.7
	Bulgaria	view_nurBG	-0.2436	-3.0
	Slovakia	view_nurSK	-0.2677	-3.6
	Lithuania	view_nurLT	-0.3128	-4.1
Health insurance companies	Czech Republic	view_iCZ	0.1970	3.0
	Slovakia	view_iSK	0.1918	2.7
	France	view_iFR	-0.3972	-4.9
	Greece	view_iEL	-0.5267	-3.6
	Italy	view_iIT	-0.2881	-3.7
	Hungary	view_iHU	0.2151	3.1
	Ireland	view_iIE	-0.2385	-2.9
	Latvia	view_iLV	0.3619	3.1
	UK	view_iUK	-0.2504	-3.3
Private sector pharmaceutical companies	Bulgaria	view_pBG	0.3506	3.1
	Hungary	view_pHU	0.4135	4.8
	Latvia	view_pLV	0.4726	3.3
	Lithuania	view_pLT	0.2246	2.8
	Portugal	view_pPT	0.3612	4.6
	Romania	view_pRO	0.4641	3.9
	Slovakia	view_pSK	0.2147	2.7
	Austria	view_pAT	-0.2287	-1.8
	Belgium	view_pBE	-0.1998	-1.9

	Denmark	view_pDK	-0.1403	-1.3
	Estonia	view_pEE	-0.2457	-1.6
	Germany	view_pDE	-0.4704	-4.5
	Luxembourg	view_pLU	-1.5619	-4.1
	Slovenia	view_pSI	-0.3205	-2.4
Academic researchers	Estonia	view_mEE	0.3569	3.5
	Denmark	view_mDK	0.3337	4.6
	Romania	view_mRO	-0.2263	-1.8

Country effects			
Country	**Label**	**Coef.**	**t-ratio**
Austria	Scale_AT	1.0000	n/a
Belgium	Scale_BE	1.0424	8.1
Bulgaria	Scale_BG	0.8356	8.1
Cyprus	Scale_CY	0.4433	5.2
Czech Republic	Scale_CZ	1.2973	8.3
Denmark	Scale_DK	1.3278	7.0
Estonia	Scale_EE	0.8200	7.3
Finland	Scale_FI	0.9690	8.2
France	Scale_FR	1.0872	7.5
Germany	Scale_DE	0.9866	9.0
Greece	Scale_EL	0.6445	8.0
Hungary	Scale_HU	1.1729	7.9
Ireland	Scale_IE	1.0443	7.1
Italy	Scale_IT	1.1090	8.2
Latvia	Scale_LV	0.5867	8.8
Lithuania	Scale_LT	0.8544	8.2
Luxembourg	Scale_LU	0.5702	5.5
Malta	Scale_MT	0.5484	7.3
Netherlands	Scale_NL	1.0042	9.5
Poland	Scale_PL	1.0022	8.6
Portugal	Scale_PT	1.3405	7.8
Romania	Scale_RO	0.6226	7.8
Slovakia	Scale_SK	1.3118	8.5
Slovenia	Scale_SI	0.6424	7.5
Spain	Scale_ES	1.1395	8.3
Sweden	Scale_SE	1.2930	8.6
UK	Scale_UK	1.3774	8.0
Survey method effects			
Online	Scale_O	1.0000	n/a
Face to Face	Scale_F	0.8855	12.0

None constant			
Country	**Label**	**Coef.**	**t-ratio**
Italy (Face)	None_IT_F	-0.8472	-5.8
Italy (Online)	None_IT_O	-0.6269	-6.8
UK	None_UK	-0.4800	-5.6
Sweden	None_SE	-0.1423	-2.5
Spain	None_ES	-0.6867	-7.3
Slovenia	None_SI	-0.4904	-3.3
Slovakia	None_SK	-0.7816	-6.7
Romania	None_RO	-1.5725	-7.9
Portugal	None_PT	-0.5074	-7.9
Poland	None_PL	-0.4753	-5.9
Netherlands	None_NL	-0.2724	-4.2
Malta	None_MT	-2.7229	-8.6
Luxembourg	None_LU	-0.5711	-3.6
Lithuania	None_LT	-1.4539	-9.6
Latvia	None_LV	-3.2232	-8.2
Ireland	None_IE	-0.7435	-7.7
Hungary	None_HU	-0.1475	-2.4
Greece	None_EL	-1.4498	-8.1
Germany (Face)	None_DE_F	-0.4714	-4.0
Germany (Online)	None_DE_O	-0.3383	-3.8
France	None_FR	-0.2219	-3.6
Finland	None_FI	-0.3317	-4.1
Estonia	None_EE	-0.3732	-4.8
Denmark	None_DK	-0.2513	-4.2
Czech Republic	None_CZ	-0.5978	-6.3
Cyprus	None_CY	-0.2221	-0.9
Bulgaria	None_BG	-2.0758	-8.9
Belgium	None_BE	-0.6640	-6.9
Austria	None_AT	-0.3650	-3.7

Appendix B: Modelling the effects of country-specific, socio-economic and attitudinal factors on preferences relating to security, surveillance and privacy

Table B.1: General latent constructs used to capture attitudes

Latent construct	Statements (manifest variables)	Measurement scale
General distrust	Indicate the level of agreement with the following statements: a) Technology has almost got out of control b) Government can generally be trusted to look after our interests c) The way one votes has no effect on what the government does d) In general business helps us more than it harms us	Scale ranging from 1 to 5, where 1 is 'Disagree strongly' and 5 is 'Agree strongly' for statements a and c and the reverse for statements b and d
Trust in institutions	How much do you trust the following institutions? • Banks • Data protection authorities • Hospitals • Large Internet-based companies such as Google or Facebook • Multinational companies • Private health insurance companies • The army • The courts of law • European Union • Media • National government	Scale ranging from 'don't trust at all' (scored as 1) to 'completely trust them' (scored as 5)
Risk taking	Please indicate the likelihood that you would engage in the described activity or behaviour: • Revealing a friend's secret to someone else • Moving to a city far away from your extended family • Leaving your young children alone at home while running an errand • Walking home alone at night in an unsafe area of town • Engaging in unprotected sex • Not returning a wallet you found that contains € [or £ or kr.] 200 • Driving a car without wearing a seat belt • Choosing a career that you truly enjoy over a more secure one • Admitting that your tastes are different from those of a friend • Passing off somebody else's work as your own • Speaking your mind about an unpopular issue in a meeting at work • Having an affair with a married man/woman	Scale ranging from 1 to 5, where 1 corresponds to 'Very Unlikely', 3 corresponds to 'Not Sure', and 5 corresponds to 'Very Likely'
General surveillance concern	Indicate the level of agreement with the following statements: • Often security is used as an excuse to impose stricter surveillance and control over the population • Public security surveillance systems are not designed to provide acceptable privacy protections • Increasing surveillance increases the risk of discrimination • Investments in security are not being particularly effective in reducing crimes	Scale ranging from 1 to 5, where 1 is 'Disagree strongly' and 5 is 'Agree strongly'

Table B.2: Context-specific latent constructs used to capture attitudes

Latent construct	Statements	Measurement scale
Travel context privacy concern	How concerned are you about the following? • Misuse of CCTV camera images by the authorities • Misuse of travel data (travel origin, destination, frequency) for tracking a person's whereabouts • Misuse of security measures for sexual or racial harassment • Sharing travel data and CCTV images across and outside the EU	Scale ranging from 1 to 5, where 1 corresponds to 'Not concerned', and 5 corresponds to 'Very concerned'
Internet context privacy concern	How concerned are you about the following? • Your information (such as age, gender, location) shared with websites or companies that you don't use • Your Internet usage information (including details of items you searched for or purchased) shared with websites or companies that you don't use (third party) • Your personal information is not handled in a legitimate way (for example, the personal information you provided when opening an account with a website is not deleted when you closed the account) • Your personal conversations on the Internet being monitored • Your Internet usage monitored by police departments in a different country	Scale ranging from 1 to 5, where 1 corresponds to 'Not concerned' at all, and 5 corresponds to 'Very concerned'
Internet security concern	To what extent do you agree with the following statements? • Most Internet websites are safe environments in which to exchange information • Most Internet websites are reliable environments in which to conduct business • Most Internet websites handle users' personal information in a competent fashion • Not using services is preferable to having personal information collected and monitored online • Too much personal information is collected and stored by websites or ISPs	Scale ranging from 1 to 5, where 1 corresponds to 'Disagree strongly', and 5 corresponds to 'Agree strongly'
Health context privacy concern	How concerned are you about the following? • Personal information (your name, address, health conditions) accessed by non-medical personnel (e.g. police) • Personal information (your name, address, health conditions) accessed by private companies (such as pharmaceutical and insurance companies) • Misuse of personal information for harassment based on race, health status, sexual orientation, etc.)	Scale ranging from 1 to 5, where 1 corresponds to 'Not concerned', and 5 corresponds to 'Very concerned'
Usefulness of health data storage	Indicate the level of agreement with the following statements: • A system that stores health information (such as your blood group, allergies, health conditions) can be useful in providing higher-quality treatments • A system that stores health-related information (such as your blood group, allergies, health conditions) can be useful in preventing health epidemics (e.g. H1N1/swine flu) • I am concerned that in a health emergency there could be an unacceptable delay due to the time spent in identifying the person needing help and their health conditions before the treatment • I'm concerned that healthcare providers (such as hospitals and health	Scale ranging from 1 to 5, where 1 is 'Disagree strongly' and 5 is 'Agree strongly'

Latent construct	Statements	Measurement scale
	insurance companies) are collecting too much personal information about me • Healthcare providers (such as hospitals and health insurance companies) are successful in preventing unauthorised access to personal information • Computer databases that contain health information (including health conditions, allergies, identification) should be protected from unauthorized access no matter how much it costs	

Table B.3: Travel model results with attitudinal effects

Model file	Travel_v56.F12		
Estimation Date	10-Apr-14		
Estimation Time	16:23:36		
Summary statistics			
Observations	60472		
Final Log Likelihood	-60588.3		
D.O.F	166		
$Rho^2(0)$	0.088		
$Rho^2(c)$	0.065		
Description	**Label**	**Coefs.**	**t-ratio**
Type of CCTV cameras			
Standard CCTV – working like a television	cam_std	1.4152	13.17
Advanced CCTV that can detect abandoned bags	cam_bag	1.5401	13.71
Advanced CCTV that can recognise suspicious movements of people	cam_sus	1.4605	13.29
Advanced CCTV that can recognise faces	cam_face	1.5820	13.85
No CCTV cameras	cam_none	0	n/a
How long CCTV camera information is stored			
CCTV information not stored for future use – only real-time monitoring	dur_rt	0.0000	n/a
CCTV information stored for 3 days	dur_3d	0.2204	7.47
CCTV information stored for 7 days	dur_7d	0.3776	11.03
CCTV information stored for 15 days	dur_15d	0.3863	11.40
CCTV information stored for 45 days	dur_45d	0.2095	7.02
Who can access CCTV camera information			
Only police departments in the [UK] have access to the camera information	acc_op	0.0000	n/a
All European police departments have access to the camera information	acc_eu	-0.1423	-7.06
All police departments worldwide have access to the camera information	acc_int	-0.2783	-11.02
Security personnel at the station			
No security personnel	per_none	0	n/a
Unarmed security personnel employed by a private company	pers_pvt	0.4949	10.19
Armed security personnel employed by a private company	pers_ta	0.4005	8.55
Unarmed police	pers_pol	0.6523	12.01
Armed police	pers_arm	0.3967	8.41
Type of security checks at the station			
People randomly selected for physical search and bag check	sec_pd	-0.2764	-10.29
People randomly selected to go through metal detector or full body scanner	sec_md	-0.0323	-1.49
No physical security checks	sec_none	0	n/a
Time to go through security checks			
10 seconds 30 seconds 1 minute 2 minutes 5 minutes	time	-0.0003	-9.20
Security surcharge on top of ticket cost			
HH Income less than €500	cost_1t4	-0.0080	-10.37
HH Income from €500 to €1,250	cost_5t6	-0.0065	-10.82
HH Income from €1,250 to €5,000	cost_7t14	-0.0044	-12.74
HH Income greater than €5,000	cost_gt14	-0.0037	-5.19
Missing Income (Low-income countries)	cost_NA_L	-0.0172	-11.32
Missing Income (Medium-income countries)	cost_NA_M	-0.0082	-7.36
Missing Income (High-income counties)	cost_NA_H	-0.0074	-3.03

Description	Label	Description	Coefs	t-ratio
Type of CCTV cameras				
Standard CCTV – working like a television	cam_std_SE	Sweden	0.2673	3.8
Advanced CCTV that can recognise faces	Camface_HU	Hungary	-0.2955	-2.9
No CCTV cameras	Nocam_BG	Bulgaria	0.4547	3.8
	Nocam_CZ	Czech Republic	0.6466	5.9
	Nocam_EL	Greece	0.5816	6.7
	Nocam_FR	France	-0.2767	-1.9
	Nocam_HU	Hungary	0.3765	3.3
	Nocam_LV	Latvia	0.4585	3.6
	Nocam_MT	Malta	0.0000	n/a
	Nocam_PL	Poland	0.3625	2.8
	Nocam_PT	Portugal	0.6734	5.5
	Nocam_SK	Slovakia	0.4772	3.7
	Nocam_male	Male	0.1788	4.9
	Nocam_1824	Age group 18–24	0.1117	1.9
	Nocam_5564	Age group 55–64	-0.1672	-3.4
How long CCTV camera information is stored				
CCTV information not stored for future use – only real-time monitoring	dur_rt_AT	Austria	0.2451	3.0
	dur_rt_EL	Greece	0.4171	5.0
	dur_rt_EE	Estonia	-0.3155	-3.3
	dur_rt_IE	Ireland	-0.1717	-2.3
CCTV information stored for 45 days	dur_45d_MT	Malta	0.0000	n/a
	dur_45d_ES	Spain	0.2710	3.7
	dur_45d_CZ	Czech Republic	-0.3835	-3.1
Who can access CCTV camera information				
acc_eu_LV	acc_eu_LV	Latvia	-0.3277	-2.9
acc_int_DE	acc_int_DE	Germany	-0.3071	-3.5
Security personnel at the station				
No security personnel	nospers_BE	Belgium	-0.1874	-2.4
	nospers_CY	Cyprus	-0.7749	-3.1
	nospers_CZ	Czech Republic	0.2311	2.4
	nospers_DE	Germany	0.3400	4.6
	nospers_ES	Spain	-0.4384	-5.4
	nospers_FR	France	-0.4735	-3.8
	nospers_HU	Hungary	0.2944	3.1
	nospers_IT	Italy	-0.1986	-2.2
Unarmed security personnel employed by a private company	perspvt_FR	France	-0.3900	-3.9
Armed security personnel employed by a private company	persta_DE	Germany	-0.5615	-5.9
	persta_EE	Estonia	0.1583	2.1
	persta_FR	France	-0.3008	-2.9
	persta_IE	Ireland	-0.2277	-3.4
	persta_UK	UK	-0.2783	-3.8
Armed police	persarm_BE	Belgium	0.2599	3.8
	persarm_FR	France	0.4078	4.1
	persarm_PL	Poland	-0.4365	-3.5
Type of security checks at the station				
No physical security checks	nosec_AT	Austria	0.2482	4.2
	nosec_CZ	Czech Republic	0.4223	4.5
	nosec_DE	Germany	0.4586	5.6
	nosec_DK	Denmark	0.2428	3.8
	nosec_ES	Spain	-0.1509	-3.0
	nosec_FR	France	-0.2047	-3.2
	nosec_IT	Italy	-0.3064	-4.5
	nosec_LV	Latvia	0.4726	4.6

	nosec_PL	Poland	0.4094	3.9
	nosec_SE	Sweden	0.2336	3.9
	nosec_SI	Slovenia	0.9382	3.3
	nosec_SK	Slovakia	0.4319	4.0
	nosec_UK	UK	-0.1435	-2.6
People randomly selected to go through metal detector or full body scanner	sec_md_BG	Bulgaria	0.2687	3.1
	sec_md_LU	Luxembourg	-0.2693	-3.6
	secmd_1824	Age group 18–24	0.0709	1.8

Country effects			
Country	**Label**	**Coef.**	**t-ratio**
Austria	Scale_AT	1.0000	n/a
Belgium	Scale_BE	1.1526	12.9
Bulgaria	Scale_BG	0.8817	7.4
Cyprus	Scale_CY	0.8509	5.8
Czech Republic	Scale_CZ	0.9993	7.1
Denmark	Scale_DK	1.1248	10.8
Estonia	Scale_EE	0.9712	12.0
Finland	Scale_FI	0.9792	12.9
France	Scale_FR	0.9477	9.2
Germany	Scale_DE	0.9702	11.0
Greece	Scale_EL	1.3950	7.7
Hungary	Scale_HU	1.1499	7.7
Ireland	Scale_IE	1.1199	13.2
Italy	Scale_IT	1.1007	11.3
Latvia	Scale_LV	0.9460	7.4
Lithuania	Scale_LT	0.7168	4.3
Luxembourg	Scale_LU	0.9069	11.2
Malta	Scale_MT	0.9682	6.9
Netherlands	Scale_NL	1.0099	11.9
Poland	Scale_PL	1.0854	7.4
Portugal	Scale_PT	0.9987	7.2
Romania	Scale_RO	0.7079	7.0
Slovakia	Scale_SK	0.8804	6.9
Slovenia	Scale_SI	0.5520	4.9
Spain	Scale_ES	1.1863	13.0
Sweden	Scale_SE	1.1101	13.0
UK	Scale_UK	1.1026	12.9
Survey method effects			
Online	Scale_O	1.0000	n/a
Face to Face	Scale_F	0.7315	11.4

None constant			
Country	**Label**	**Coef.**	**t-ratio**
Italy (Face)	None_IT_F	-1.0913	-5.9
Italy (Online)	None_IT_O	-0.8432	-6.1
UK	None_UK	-0.7603	-6.3
Sweden	None_SE	0.1824	1.7
Spain	None_ES	-0.8730	-6.8
Slovenia	None_SI	-0.1604	-0.8
Slovakia	None_SK	-0.6658	-4.7
Romania	None_RO	-1.6206	-7.7
Portugal	None_PT	-0.6892	-5.0
Poland	None_PL	-0.2999	-2.4
Netherlands	None_NL	-0.5097	-4.5
Malta	None_MT	-1.4998	-6.8
Luxembourg	None_LU	-0.5638	-4.6
Lithuania	None_LT	-1.2617	-4.3
Latvia	None_LV	-2.3928	-9.3
Ireland	None_IE	-0.6438	-5.6
Hungary	None_HU	0.0503	0.4
Greece	None_EL	-0.8947	-6.6
Germany (Face)	None_DE_F	-0.4588	-3.2
Germany (Online)	None_DE_O	-0.2058	-1.7
France	None_FR	-1.0010	-5.7
Finland	None_FI	-0.0447	-0.4
Estonia	None_EE	-0.9937	-7.3
Denmark	None_DK	0.3963	3.7
Czech Republic	None_CZ	-0.1211	-1.0
Cyprus	None_CY	-1.1329	-5.6
Bulgaria	None_BG	-2.4182	-9.1
Belgium	None_BE	-0.3954	-3.5
Austria	None_AT	-0.2546	-2.3

None constant			
Attitudinal attribute	**Label**	**Coef.**	**t-ratio**
Concern for privacy while travelling (all reported income levels)			
Misuse of CCTV camera images by authorities	bconcern_1	0.0813	5.1
Misuse of travel data for tracking a person's whereabouts	bconcern_2	0.0593	3.5
Misuse of security measures for sexual or racial harassment	bconcern_3	-0.1104	-7.2
Sharing travel data and CCTV images across and outside the EU	bconcern_4	0.0561	4.0
Concern for privacy while travelling (income level not reported)			
Misuse of CCTV camera images by authorities	bcon1_na	0.8055	4.8
Misuse of travel data for tracking a person's whereabouts	bcon2_na	0.5500	2.9
Misuse of security measures for sexual or racial harassment	bcon3_na	0.1031	0.7
Sharing travel data and CCTV images across and outside the EU	bcon4_na	-0.0872	-0.6

General distrust (all reported income levels)			
Technology has almost got out of control	bdist_1	0.0000	n/a
Government can generally be trusted to look after our interests	bdist_2	0.1041	9.0
The way one votes has no effect on what the government does	bdist_3	0.0036	0.4
In general business helps us more than it harms us	bdist_4	0.0550	4.7
General distrust (income level not reported)			
Technology has almost got out of control	bdis1_na	0.3640	4.3
Government can generally be trusted to look after our interests	bdis2_na	0.4453	3.0
The way one votes has no effect on what the government does	bdis3_na	0.2001	1.4
In general business helps us more than it harms us	bdis4_na	0.3797	3.4
Effectiveness of surveillance measures (all reported income levels)			
Often security is used an excuse to impose stricter surveillance and control over the population	bscon_1	0.1450	9.7
Public security surveillance systems are not designed to provide acceptable privacy protections	bscon_2	0.0556	4.1
Increasing surveillance increases the risk of discrimination	bscon_3	0.0592	5.0
Investments in security are not being particularly effective in reducing crimes	bscon_4	0.0310	2.8
Effectiveness of surveillance measures (income level not reported)			
Often security is used an excuse to impose stricter surveillance and control over the population	bscon1_na	0.2953	2.5
Public security surveillance systems are not designed to provide acceptable privacy protections	bscon2_na	0.2286	2.3
Increasing surveillance increases the risk of discrimination	bscon3_na	0.6842	6.3
Investments in security are not being particularly effective in reducing crimes	bscon4_na	0.2770	2.6

Description	Label	Description	Coefficients	t-ratio
Type of CCTV cameras				
no CCTV	bnocam_I1	Misuse of CCTV camera images by authorities	0.0514	2.2
	bnocam_I2	Misuse of travel data for tracking a person's whereabouts	0.0731	2.9
	bnocam_I3	Misuse of security measures for sexual or racial harassment	-0.0818	-3.9
	bnocam_I4	Sharing travel data and CCTV images across and outside the EU	0.0000	n/a
	nCSI1	Often security is used an excuse to impose stricter surveillance and control over the population	0.0900	5.0
	nCSI3	Increasing surveillance increases the risk of discrimination	0.0625	3.6
Security personnel at the station				
No security personnel	bnspers_I2	Misuse of CCTV camera images by authorities	0.0577	4.4

Table B.4: Internet model results with attitudinal effects

Description	Label	Description	Coefficients	t-ratio
Type of Internet usage information stored				
No information will be stored	nodata_BG	Bulgaria	-0.6090	-4.2
	nodata_FI	Finland	0.2818	2.7
	nodata_LV	Latvia	-0.6816	-5.0
	nodata_LT	Lithuania	-0.8871	-5.4
Website you have visited	data_1_18	Age 18–24	0.2818	4.5
All Internet activities	alldata_FI	Finland	-0.3530	-3.1
	alldata_IE	Ireland	-0.4063	-3.2
How long Internet data are stored				
1 year	dur_1y_LV	Latvia	0.3456	2.4
Who has access to Internet information				
Worldwide	acc_int_LU	Luxembourg	-0.2405	-2.6
	acc_int_SI	Slovenia	0.4946	4.0
When ISP can allow continuous surveillance of its Internet users by the police				
Any time without a warrant	cond_1_LT	Lithuania	-1.0610	-4.0
Only with a warrant	cond_2_DK	Denmark	0.3741	4.3
	cond_2_ES	Spain	0.5313	5.2
Without a warrant but only under government declared state of emergency	cond_3_LT	Lithuania	-0.8997	-4.7
	cond_3_55	Age 55–64	-0.1215	-2.6
Never	cond_4_65	Age over 65	-0.1217	-2.6
	cond_4_MT	Malta	-0.8110	-3.5
Services offered to improve online privacy				
ISP will not offer any service to improve your online privacy	serv_1_SK	Slovakia	0.3622	3.4
	serv_1_EE	Estonia	-0.2707	-3.6
	serv_1_CZ	Czech Republic	0.6194	5.7
	serv_1_BE	Belgium	-0.3052	-3.4
	serv_1_65	Age over 65	-0.1997	-3.8
	serv_1_man	Male	0.2495	6.8
None of these options				
	none_18	Age 18–24	-0.3918	-10.5
	none_25	Age 25–34	-0.1525	-5.4

Country effects			
Country	**Label**	**Coef.**	**t-ratio**
Austria	Scale_AT	1.0000	n/a
Belgium	Scale_BE	0.8036	21.9
Bulgaria	Scale_BG	0.6607	11.2
Cyprus	Scale_CY	0.4634	9.5
Czech Republic	Scale_CZ	0.6729	12.1
Denmark	Scale_DK	0.8892	20.3
Estonia	Scale_EE	1.0000	n/a
Finland	Scale_FI	0.8556	18.7
France	Scale_FR	0.8329	22.4
Germany	Scale_DE	1.0000	n/a
Greece	Scale_EL	0.5390	10.8
Hungary	Scale_HU	0.7118	12.2

None constant			
Country	**Label**	**Coef.**	**t-ratio**
Italy (Face)	None_IT_F	-0.9237	-5.4
Italy (Online)	None_IT_O	-0.6703	-4.4
UK	None_UK	-0.7992	-5.8
Sweden	None_SE	-0.1906	-1.4
Spain	None_ES	-0.5806	-3.8
Slovenia	None_SI	-0.5969	-3.6
Slovakia	None_SK	-0.7708	-5.2
Romania	None_RO	-2.1309	-10.0
Portugal	None_PT	-0.0295	-0.1
Poland	None_PL	-0.4448	-2.7
Netherlands	None_NL	-0.6777	-5.1
Malta	None_MT	-3.1422	-9.3

Ireland	Scale_IE	0.7256	19.6
Italy	Scale_IT	0.7146	17.1
Latvia	Scale_LV	0.6850	11.9
Lithuania	Scale_LT	0.5574	10.3
Luxembourg	Scale_LU	1.0000	n/a
Malta	Scale_MT	0.3962	7.5
Netherlands	Scale_NL	1.0000	n/a
Poland	Scale_PL	0.6104	11.7
Portugal	Scale_PT	0.4207	8.9
Romania	Scale_RO	0.4458	9.2
Slovakia	Scale_SK	0.7418	12.6
Slovenia	Scale_SI	0.5563	11.3
Spain	Scale_ES	0.6291	18.7
Sweden	Scale_SE	0.9656	21.6
UK	Scale_UK	0.8936	22.7
Survey method effects			
Online	Scale_O	1.0000	n/a
Face to Face	Scale_F	0.7760	16.7

Luxembourg	None_LU	-0.5842	-4.2
Lithuania	None_LT	-3.0983	-13.8
Latvia	None_LV	-4.5011	-17.7
Ireland	None_IE	-0.7721	-5.4
Hungary	None_HU	-0.3023	-1.9
Greece	None_EL	-1.9299	-10.8
Germany (Face)	None_DE_F	-0.1431	-0.9
Germany (Online)	None_DE_O	-0.3702	-2.7
France	None_FR	-0.5216	-3.7
Finland	None_FI	-0.2674	-1.9
Estonia	None_EE	-0.8274	-6.1
Denmark	None_DK	-0.2191	-1.6
Czech Republic	None_CZ	-0.8731	-5.6
Cyprus	None_CY	-0.7415	-3.7
Bulgaria	None_BG	-2.5908	-14.2
Belgium	None_BE	-0.8488	-6.1
Austria	None_AT	-0.5149	-3.8

None constant			
Attitudinal attribute	**Label**	**Coef.**	**t-ratio**
Concern for privacy while using the Internet (all reported income levels)			
Personal information shared with third-party websites or companies	bconcern_1	0.0599	3.9
Internet usage information shared with third-party websites or companies	bconcern_2	0.0484	2.6
Personal information is not handled in a legitimate way	bconcern_3	-0.1421	-8.1
Internet usage monitored by police departments in other countries	bconcern_5	0.1381	11.1
Concern for privacy while using the Internet (income level not reported)			
Personal information shared with third-party websites or companies	bcon1_na	0.9856	4.1
Internet usage information shared with third-party websites or companies	bcon2_na	0.7665	3.2
Personal information is not handled in a legitimate way	bcon3_na	-0.4534	-2.3
Internet usage monitored by police departments in other countries	bcon5_na	0.9637	5.6
General distrust (all reported income levels)			
Government can generally be trusted to look after our interests	bdist_2	0.1748	14.6
The way one votes has no effect on what the government does	bdist_3	0.0086	1.0
In general business helps us more than it harms us	bdist_4	0.0674	5.7
General distrust (income level not reported)			
In general business helps us more than it harms us	bdis4_na	0.9522	6.8
Effectiveness of online protection (all reported income levels)			
Most Internet websites are safe environments in which to exchange information	bsafe_1	0.0483	3.0
Most Internet websites handle users' personal information in a competent fashion	bsafe_3	0.0997	5.8
Not using services is preferable to having personal information collected and monitored online	bsafe_4	0.0951	6.4
Too much personal information is collected and stored by websites or ISPs	bsafe_5	0.0847	5.6
Effectiveness of online protection (income level not reported)			
Most Internet websites are safe environments in which to exchange information	bsafe1_na	0.6706	4.1
Most Internet websites are reliable environments in which to conduct business	bsafe2_na	0.4091	2.9
Most Internet websites handle users' personal information in a competent fashion	bsafe3_na	0.9110	7.0
Not using services is preferable to having personal information collected and monitored online	bsafe4_na	0.4494	2.5
Too much personal information is collected and stored by websites or ISP	bsafe5_na	0.6930	4.1

Description	Label	Description	Coefs.	t-ratio
Type of Internet usage information stored				
No information will be stored	nodata_cI2	Internet usage information shared with third-party websites or companies	0.1258	5.3
	nodata_cI3	Personal information is not handled in a legitimate way	-0.0641	-2.6
	nodata_cI5	Internet usage monitored by police departments in other countries	0.0903	5.2
	nodata_dI1	Technology has almost got out of control	-0.0470	-3.0
	nodata_dI2	Government can generally be trusted to look after our interests	0.1567	9.0
	nodata_sI1	Most Internet websites are safe environments in which to exchange information	0.0747	3.5
	nodata_sI3	Most Internet websites handle users' personal information in a competent fashion	0.0568	2.4
	nodata_sI4	Not using services is preferable to having personal information collected and monitored online	0.0712	3.5
	nodata_sI5	Too much personal information is collected and stored by websites or ISPs	0.0679	3.0
When ISP can allow continuous surveillance of its Internet users by the police				
Never	cond1_cI2	Internet usage information shared with third-party websites or companies	-0.1136	-4.4
	cond1_cI3	Personal information is not handled in a legitimate way	0.0592	2.3
	cond1_cI5	Internet usage monitored by police departments in other countries	-0.0662	-3.5
	cond1_dI1	Technology has almost got out of control	0.0901	5.0
	cond1_dI2	Government can generally be trusted to look after our interests	-0.0715	-3.8
	cond1_sI1	Most Internet websites are safe environments in which to exchange information	-0.0517	-2.2
	cond1_sI3	Most Internet websites handle users' personal information in a competent fashion	-0.0607	-2.4
	cond1_sI4	Not using services is preferable to having personal information collected and monitored online	-0.0761	-3.9
Services offered to improve online privacy				
ISP will not offer any service to improve online privacy	serv1_cI3	Personal information is not handled in a legitimate way	-0.0938	-4.7
	serv1_cI5	Internet usage monitored by police departments in other countries	0.0466	2.7
ISP will warn you which sites do not meet your desired level of privacy	serv3_sI4	Not using services is preferable to having personal information collected and monitored online	0.0672	4.0

Table B.5: Health model results with attitudinal effects

Model file	Health_v31.F12		
Estimation Date	28-Feb-14		
Estimation Time	15:34:24		
Summary statistics			
Observations	94606		
Final Log Likelihood	-93598.6		
D.O.F	117		
$Rho^2(0)$	0.099		
$Rho^2(c)$	0.079		
Description	**Label**	**Coefficient**	**t-ratio**
What information is stored on the device/system			
Basic health status	data_1	0.0000	n/a
Basic health status + Identification	data_2	0.1855	5.62
Basic health status + Identification + Lifelong health conditions	data_3	0.2830	7.08
Basic health status + Identification + Lifelong health conditions + All other health conditions and medical history	data_4	0.0935	3.24
Who can access the information			
Only doctors and nurses	acc_1	0.0000	n/a
Doctors, nurses, and paramedics	acc_2	0.1061	3.16
Doctors, nurses, paramedics and fire and rescue	acc_3	-0.0512	-1.57
In which countries your information can be accessed?			
Only in the home country	acch_ter	0.0000	n/a
Across Europe (EU)	acch_eu	0.0440	2.50
Worldwide	acch_int	-0.2939	-8.41
Who else can view this information apart from the medical specialists?			
No one	view_non	0.0000	n/a
Immediate family	view_fam	-0.0771	-1.88
Nurses providing home care	view_nur	0.0000	n/a
Health insurance companies	view_ins	-0.0555	-1.31
Private sector pharmaceutical companies	view_pri	-0.4726	-5.19
Academic researchers	view_med	-0.6569	-12.71
Cost			
HH income less than €500	cost1t4	-0.0043	-13.76
HH income from €500 to €1500	cost5t8	-0.0038	-13.06
HH income from €1500 to €3000	cost9t11	-0.0033	-14.40
HH income from €3000 to €9000	cost12t18	-0.0029	-11.16
HH income greater than €9000	cost19t21	-0.0018	-3.41
Missing income	costNA	-0.0049	-12.68

Country effects			
Country	**Label**	**Coef.**	**t-ratio**
Austria	Scale_AT	1	n/a
Belgium	Scale_BE	1.0595	9.9
Bulgaria	Scale_BG	0.834	10.0
Cyprus	Scale_CY	0.4828	5.9
Czech Republic	Scale_CZ	1.1258	8.3
Denmark	Scale_DK	1.2319	10.4
Estonia	Scale_EE	0.9374	11.2
Finland	Scale_FI	1.0605	10.2
France	Scale_FR	1.0575	10.4
Germany	Scale_DE	0.8466	8.9

None constant			
Country	**Label**	**Coef.**	**t-ratio**
Italy (Face)	None_IT_F	1.3321	8.1
Italy (Online)	None_IT_O	1.4333	9.4
UK	None_UK	1.6716	12.3
Sweden	None_SE	2.0391	13.6
Spain	None_ES	1.5846	10.7
Slovenia	None_SI	1.6674	10.7
Slovakia	None_SK	1.313	8.7
Romania	None_RO	0.6758	5.0
Portugal	None_PT	1.7255	14.7
Poland	None_PL	1.4729	14.5

Greece	Scale_EL	0.8584	8.4
Hungary	Scale_HU	1.1652	9.5
Ireland	Scale_IE	1.036	8.8
Italy	Scale_IT	1.0163	9.9
Latvia	Scale_LV	0.6921	10.7
Lithuania	Scale_LT	0.8845	9.6
Luxembourg	Scale_LU	0.8845	9.1
Malta	Scale_MT	0.5918	8.5
Netherlands	Scale_NL	1.0898	11.7
Poland	Scale_PL	0.9887	8.8
Portugal	Scale_PT	1.2147	9.5
Romania	Scale_RO	0.8325	9.1
Slovakia	Scale_SK	1.3216	8.9
Slovenia	Scale_SI	0.6406	8.8
Spain	Scale_ES	1.0623	12.3
Sweden	Scale_SE	1.1241	10.1
UK	Scale_UK	1.1929	9.7
Survey method effects			
Online	Scale_O	1	n/a
Face to Face	Scale_F	0.7556	17.2

Netherlands	None_NL	1.7678	14.6
Malta	None_MT	-0.4757	-2.8
Luxembourg	None_LU	1.5228	12.1
Lithuania	None_LT	0.6603	5.5
Latvia	None_LV	-1.1984	-5.2
Ireland	None_IE	1.3868	10.9
Hungary	None_HU	2.1356	12.6
Greece	None_EL	0.5337	4.9
Germany (Face)	None_DE_F	1.7101	10.8
Germany (Online)	None_DE_O	1.8861	9.7
France	None_FR	1.9161	13.9
Finland	None_FI	2.0077	13.2
Estonia	None_EE	1.8395	13.5
Denmark	None_DK	2.1271	13.0
Czech Republic	None_CZ	1.5661	11.5
Cyprus	None_CY	1.9425	8.2
Bulgaria	None_BG	-0.2374	-1.3
Belgium	None_BE	1.5333	11.3
Austria	None_AT	1.7693	11.6

None constant			
Attitudinal attribute	**Label**	**Coef.**	**t-ratio**
Concern for privacy in the health context (all reported income levels)			
Personal information (your name, address, health conditions) accessed by non-medical personnel (e.g. police) without your consent.	bconcern_1	0.0975	6.1
Personal information (your name, address, health conditions) accessed by private companies (such as pharmaceutical and insurance companies) without your consent	bconcern_2	0.0553	3.6
Misuse of personal information for harassment based on race, health status, sexual orientation, etc.	bconcern_3	-0.0769	-5.0
Concern for privacy in the health context (income level not reported)			
Personal information (your name, address, health conditions) accessed by non-medical personnel (e.g. police) without your consent	bcon1_na	0.3414	1.5
Personal information (your name, address, health conditions) accessed by private companies (such as pharmaceutical and insurance companies) without your consent	bcon2_na	0.563	2.2
Misuse of personal information for harassment based on race, health status, sexual orientation, etc.	bcon3_na	0.3053	2.3
General distrust (all reported income levels)			
Technology has almost got out of control	bdist_1	0.0141	1.3
Government can generally be trusted to look after our interests	bdist_2	-0.0828	-5.8
The way one votes has no effect on what the government does	bdist_3	0.0381	4.5
In general business helps us more than it harms us	bdist_4	-0.0205	-2.1
General distrust (income level not reported)			
Technology has almost got out of control	bdis1_na	0.4334	4.9
The way one votes has no effect on what the government does	bdis3_na	0.1246	1.1
Usefulness of health data storage (all reported income levels)			
A system that stores health information (such as your blood group, allergies, health conditions) can be useful in providing higher-quality treatments	bhstat_1	-0.2565	-11.5
A system that stores health-related information (such as your blood group, allergies, health conditions) can be useful in preventing health epidemics (e.g. H1N1/swine flu)	bhstat_2	-0.1828	-12.0

I am concerned that in a health emergency there could be an unacceptable delay due to the time spent in identifying the person needing help and their health conditions before the treatment	bhstat_3	-0.1674	-11.7
I'm concerned that healthcare providers (such as hospitals and health insurance companies) are collecting too much personal information about me	bhstat_4	0.0998	8.7
Healthcare providers (such as hospitals and health insurance companies) are successful in preventing unauthorised access to personal information	bhstat_5	-0.0717	-6.2
Usefulness of health data storage (income level not reported)			
A system that stores health information (such as your blood group, allergies, health conditions) can be useful in providing higher-quality treatments	bhsta1_na	-0.8653	-4.7
A system that stores health-related information (such as your blood group, allergies, health conditions) can be useful in preventing health epidemics (e.g. H1N1/swine flu)	bhsta2_na	-0.5108	-3.6
I am concerned that in a health emergency there could be an unacceptable delay due to the time spent in identifying the person needing help and their health conditions before the treatment	bhsta3_na	-0.1724	-1.4
I'm concerned that healthcare providers (such as hospitals and health insurance companies) are collecting too much personal information about me	bhsta4_na	0.5778	4.4
Healthcare providers (such as hospitals and health insurance companies) are successful in preventing unauthorised access to personal information	bhsta5_na	0.1551	2.2
Computer databases that contain health information (including health conditions, allergies, identification) should be protected from unauthorized access no matter how much it costs	bhsta6_na	0.483	3.9

Description	Label	Description	Coeffs	t-ratio
What information is stored on the device/system				
Basic health data	data_1c2	Personal information (your name, address, health conditions) accessed by private companies (such as pharmaceutical and insurance companies) without your consent	0.0404	4.6
Who can access the information				
Only doctors and nurses	acc_1c1	Personal information (your name, address, health conditions) accessed by non-medical personnel (e.g. police) without your consent	0.0388	3.8
	acc_1c3	Misuse of personal information for harassment based on race, health status, sexual orientation, etc.	-0.0277	-2.6
In which countries your information can be accessed?				
Only in the home country	acch_tc1	Personal information (your name, address, health conditions) accessed by non-medical personnel (e.g. police) without your consent.	-0.1534	-4.5
Worldwide	acch_ic2	Personal information (your name, address, health conditions) accessed by private companies (such as pharmaceutical and insurance companies) without your consent	0.0306	3.6
Who else can view this information apart from the medical specialists?				
No one	view_nc1	Personal information (your name, address, health conditions) accessed by non-medical personnel (e.g. police) without your consent	-0.0502	-3.2
	view_nc2	Personal information (your name, address, health conditions) accessed by private companies (such as pharmaceutical and insurance companies) without your consent	0.0672	5.0

Immediate family	view_fc2	Personal information (your name, address, health conditions) accessed by private companies (such as pharmaceutical and insurance companies) without your consent	0.0223	2.1
Health insurance companies	view_ic2	Personal information (your name, address, health conditions) accessed by private companies (such as pharmaceutical and insurance companies) without your consent	-0.0949	-7.7
Private sector pharmaceutical companies	view_pc1	Personal information (your name, address, health conditions) accessed by non-medical personnel (e.g. police) without your consent	0.0784	4.6
	view_pc2	Personal information (your name, address, health conditions) accessed by private companies (such as pharmaceutical and insurance companies) without your consent	-0.2029	-8.8
	view_pc3	Misuse of personal information for harassment based on race, health status, sexual orientation, etc.	0.0334	2.4
Academic researchers	view_mc2	Personal information (your name, address, health conditions) accessed by private companies (such as pharmaceutical and insurance companies) without your consent	0.0278	2.5

Appendix C: Structural equation model results

Table C.1: Travel results

Number of Observations	12,099
Log-Likelihood	-190105.43

		Coef.	Std. err	z	P>|z|	95% CI	
Variable		**Factor Loadings (Privacy concern while travelling in a metro/train)**					
Iconcern_1	Misuse of CCTV camera images Iconcern_1 (constrained)	1.0000					
Iconcern_2	Misuse of travel data Iconcern_2	1.3018	0.0335	38.91	0.0000	1.2362	1.3674
Iconern_3	Misuse of security measures Iconcern_3	0.8264	0.0180	45.90	0.0000	0.7911	0.8617
Iconern_4	Sharing travel data and CCTV images Iconcern_4	0.8826	0.0195	45.24	0.0000	0.8444	0.9209
		Factor Loadings (Concern for effectiveness of surveillance measures)					
Isconcern_1	Security is used as an excuse to impose stricter surveillance Isurv_1	1.0000					
Isconern_2	Public security surveillance systems are not designed to provide acceptable privacy protections Isurv_2	1.0059	0.0283	35.57	0.0000	0.9505	1.0613
Isconern_3	Increasing surveillance increases the risk of discrimination Isurv_3	0.9241	0.0269	34.40	0.0000	0.8714	0.9768
Isconcern_4	Investment in security are not being particularly effective in reducing crimes Isurv_4	0.6819	0.0207	32.90	0.0000	0.6412	0.7225
		Factor Loadings (Westin's Distrust)					
Itech	Q31_1 Distrust(constrained)	1.0000					
Igovern	Q31_2 Distrust	0.6872	0.0397	17.30	0.0000	0.6094	0.7651
Ivote	Q31_3 Distrust	0.6728	0.0362	18.58	0.0000	0.6018	0.7437
Ibus	Q31_4 Distrust	0.2493	0.0293	8.51	0.0000	0.1919	0.3067
		Latent Variable (Privacy concern while travelling in a metro/train)					
Privacy Concern	<-						

	age	-0.0221	0.0022	-9.95	0.0000	-0.0265	-0.0178
	HHIncome	-0.0003	0.0000	-14.71	0.0000	-0.0004	-0.0003
	HHIncNA	0.2267	0.1224	1.85	0.0640	-0.0131	0.4665
		Latent Variable (Concern for effectiveness of surveillance measures)					
Surveillance Concern	<-						
	HHIncome	-0.0002	0.0000	-13.86	0.0000	-0.0002	-0.0001
	HHIncNA	0.1187	0.0626	1.90	0.0580	-0.0040	0.2413
	male	0.2264	0.0377	6.01	0.0000	0.1526	0.3003
		Latent Variable (Distrust)					
Distrust	<-						
	age	0.0019	0.0009	2.17	0.0300	0.0002	0.0036
	HHIncome	-0.0001	0.0000	-9.90	0.0000	-0.0001	-0.0001
	HHIncNA	-0.1622	0.0469	-3.46	0.0010	-0.2542	-0.0703
	highfreq	-0.1527	0.0364	-4.19	0.0000	-0.2241	-0.0813
	male	-0.1048	0.0299	-3.50	0.0000	-0.1634	-0.0462
		Indicator Thresholds					
Iconcern_1	|						
	/cut1	-3.3708	0.1313	-25.67	0.0000	-3.6282	-3.1135
	/cut2	-0.8477	0.1241	-6.83	0.0000	-1.0910	-0.6045
	/cut3	1.7292	0.1255	13.78	0.0000	1.4832	1.9752
	/cut4	4.3242	0.1376	31.42	0.0000	4.0545	4.5939
Iconcern_2	|						
	/cut1	-4.9568	0.1815	-27.31	0.0000	-5.3126	-4.6010
	/cut2	-1.5612	0.1622	-9.63	0.0000	-1.8791	-1.2433
	/cut3	1.7431	0.1625	10.73	0.0000	1.4247	2.0616
	/cut4	5.0851	0.1829	27.81	0.0000	4.7267	5.4435
Iconcern_3	|						
	/cut1	-3.2017	0.1098	-29.17	0.0000	-3.4168	-2.9865
	/cut2	-1.0559	0.1036	-10.19	0.0000	-1.2590	-0.8529
	/cut3	1.1523	0.1035	11.13	0.0000	0.9493	1.3552
	/cut4	3.3086	0.1107	29.89	0.0000	3.0916	3.5256
Iconcern_4	|						
	/cut1	-3.6056	0.1180	-30.54	0.0000	-3.8370	-3.3743
	/cut2	-1.2955	0.1105	-11.72	0.0000	-1.5121	-1.0788
	/cut3	1.1335	0.1103	10.28	0.0000	0.9174	1.3497
	/cut4	3.4718	0.1183	29.34	0.0000	3.2399	3.7037
Isconcern_1	|						

	/cut1	-4.0734	0.0676	-60.22	0.0000	-4.2060	-3.9408
	/cut2	-2.2668	0.0492	-46.10	0.0000	-2.3632	-2.1705
	/cut3	-0.2211	0.0406	-5.45	0.0000	-0.3007	-0.1416
	/cut4	2.0901	0.0488	42.84	0.0000	1.9945	2.1857
Isconcern_2	|						
	/cut1	-4.6297	0.0771	-60.05	0.0000	-4.7808	-4.4786
	/cut2	-2.4747	0.0516	-47.95	0.0000	-2.5758	-2.3735
	/cut3	0.1287	0.0409	3.14	0.0020	0.0485	0.2090
	/cut4	2.5184	0.0522	48.23	0.0000	2.4161	2.6207
Isconcern_3	|						
	/cut1	-3.0573	0.0538	-56.83	0.0000	-3.1627	-2.9518
	/cut2	-1.2869	0.0414	-31.10	0.0000	-1.3680	-1.2058
	/cut3	0.5758	0.0387	14.89	0.0000	0.5000	0.6516
	/cut4	2.7260	0.0512	53.27	0.0000	2.6257	2.8262
Isconcern_4	|						
	/cut1	-3.1844	0.0492	-64.69	0.0000	-3.2809	-3.0879
	/cut2	-1.2727	0.0341	-37.37	0.0000	-1.3394	-1.2059
	/cut3	0.2686	0.0310	8.67	0.0000	0.2079	0.3293
	/cut4	2.0452	0.0380	53.86	0.0000	1.9708	2.1197
Itech	|						
	/cut1	-2.6334	0.0594	-44.33	0.0000	-2.7498	-2.5170
	/cut2	-1.4240	0.0527	-27.01	0.0000	-1.5273	-1.3207
	/cut3	0.2549	0.0507	5.03	0.0000	0.1556	0.3541
	/cut4	1.9047	0.0567	33.60	0.0000	1.7936	2.0158
Igovern	|						
	/cut1	-2.9990	0.0551	-54.46	0.0000	-3.1069	-2.8911
	/cut2	-1.2335	0.0418	-29.52	0.0000	-1.3154	-1.1516
	/cut3	0.0778	0.0380	2.05	0.0410	0.0032	0.1524
	/cut4	1.2505	0.0391	31.99	0.0000	1.1739	1.3271
Ivote	|						
	/cut1	-2.2237	0.0442	-50.25	0.0000	-2.3104	-2.1370
	/cut2	-1.1031	0.0386	-28.57	0.0000	-1.1788	-1.0274
	/cut3	-0.0366	0.0368	-0.99	0.3210	-0.1088	0.0356
	/cut4	1.1221	0.0387	29.03	0.0000	1.0463	1.1978
Ibus	|						
	/cut1	-2.0716	0.0323	-64.15	0.0000	-2.1349	-2.0083
	/cut2	-0.5180	0.0233	-22.22	0.0000	-0.5637	-0.4723
	/cut3	1.3549	0.0259	52.25	0.0000	1.3041	1.4057

/cut4	2.5698	0.0380	67.70	0.0000	2.4954	2.6442
	Variance and Covariance					
var(e.Concern)	17.9835	0.6305	28.52	0.0000	16.79	19.2627
var(e.SConcern)	3.5773	0.1496	23.91	0.0000	3.30	3.8829
var(e.Distrust)	0.8690	0.0629	13.81	0.0000	0.75	1.0015
cov(e.Concern,e.SConcern)	3.5885	0.1318	27.22	0.0000	3.3301	3.8469
cov(e.Concern,e.Distrust)	1.3924	0.0868	16.04	0.0000	1.2223	1.5625
cov(e.SConcern,e.Distrust)	1.3118	0.0558	23.49	0.0000	1.2023	1.4212
Correlation (e.Concern, e.Sconcern)	**0.447**					
Correlation (e.Concern, e.Distrust)	**0.352**					
Correlation (e.Sconcern, e.Distrust)	**0.744**					

Table C.2: Internet results

Number of Observations 14,865
Log-Likelihood -268351.99

		Coef.	Std. err	z	P>|z|	95% CI	
Variable		**Factor Loadings (Privacy concern while using Internet)**					
Iconcern_1	Personal information shared with websites or companies that you don't use Iconcern_1 (constrained)	1.0000					
Iconcern_2	Internet usage information shared with websites or companies that you don't use Iconcern_2	1.2434	0.0239	51.95	0.0000	1.1965	1.2903
Iconern_3	Personal information is not handled in a legitimate way Iconcern_3	1.0008	0.0213	47.10	0.0000	0.9591	1.0424
Iconern_4	Private conversations being monitored Iconcern_4	0.7585	0.0165	46.01	0.0000	0.7262	0.7908
Iconcern_5	Internet usage information monitored by police departments in a different country Iconcern_5	0.6584	0.0140	47.12	0.0000	0.6310	0.6858
		Factor Loadings (Concern for safety while using Internet)					
Isconcern_1	Most Internet websites are not safe to exchange information with others Isurv_1	1.0000					
Isconern_2	Most Internet websites are not reliable to conduct business transactions Isurv_2	1.2731	0.0352	36.19	0.0000	1.2041	1.3420
Isconern_3	Most Internet websites don't handle personal information submitted by users in a						

	competent fashion Isurv_3	0.9119	0.0205	44.52	0.0000	0.8717	0.9520
Isconcern_4	I would rather not use certain services than giving out my personal information Isurv_4	0.1002	0.0069	14.62	0.0000	0.0868	0.1136
Isconcern_5	I am concerned that too much personal information is collected and stored by ISPs Isurv_5	0.1547	0.0072	21.41	0.0000	0.1406	0.1689
		Factor Loadings (Westin's Distrust)					
Itech	Q31_1 Distrust(constrained)	1.0000					
Igovern	Q31_2 Distrust	3.9509	0.4205	9.40	0.0000	3.1268	4.7750
Ivote	Q31_3 Distrust	0.6271	0.0699	8.97	0.0000	0.4901	0.7640
Ibus	Q31_4 Distrust	2.0925	0.1936	10.81	0.0000	1.7131	2.4720
		Latent Variable (Privacy concern while travelling in a metro/train)					
Privacy Concern	<-						
	age	-0.0124	0.0020	-6.19	0.0000	-0.0163	-0.0085
	HHIncome	-0.0001	0.0000	-6.95	0.0000	-0.0002	-0.0001
	HHIncNA	-0.3990	0.0954	-4.18	0.0000	-0.5860	-0.2119
	hfreq	0.3095	0.0710	4.36	0.0000	0.1703	0.4488
	highedu	0.4829	0.0681	7.09	0.0000	0.3494	0.6164
		Latent Variable (Concern for effectiveness of surveillance measures)					
Security Concern	<-						
	HHIncome	0.0000	0.0000	0.66	0.5060	0.0000	0.0000
	HHIncNA	-0.1979	0.0757	-2.61	0.0090	-0.3463	-0.0495
	hfreq	-0.1078	0.0559	-1.93	0.0540	-0.2173	0.0018
	highedu	0.3929	0.0519	7.57	0.0000	0.2912	0.4947
	male	0.0027	0.0485	0.06	0.9550	-0.0923	0.0977
	worker	-0.1490	0.0474	-3.14	0.0020	-0.2420	-0.0561
		Latent Variable (Distrust)					
Distrust	<-						
	age	0.0001	0.0003	0.20	0.8380	-0.0005	0.0006
	HHIncome	0.0000	0.0000	-6.91	0.0000	0.0000	0.0000
	HHIncNA	-0.0661	0.0156	-4.24	0.0000	-0.0967	-0.0356
	hfreq	0.0634	0.0115	5.50	0.0000	0.0409	0.0860
	male	-0.0009	0.0093	-0.09	0.9270	-0.0191	0.0174

		Indicator Thresholds					
Iconcern_1	|						
	/cut1	-5.7820	0.1271	-45.50	0.0000	-6.0311	-5.5330
	/cut2	-3.5838	0.1143	-31.36	0.0000	-3.8078	-3.3598
	/cut3	-1.0509	0.1068	-9.84	0.0000	-1.2602	-0.8415
	/cut4	1.6855	0.1078	15.64	0.0000	1.4743	1.8967
Iconcern_2	|						
	/cut1	-7.3055	0.1690	-43.24	0.0000	-7.6367	-6.9744
	/cut2	-4.6631	0.1469	-31.74	0.0000	-4.9511	-4.3751
	/cut3	-1.5340	0.1328	-11.55	0.0000	-1.7942	-1.2737
	/cut4	1.8850	0.1339	14.07	0.0000	1.6224	2.1475
Iconcern_3	|						
	/cut1	-6.7213	0.1362	-49.36	0.0000	-6.9882	-6.4544
	/cut2	-4.4399	0.1189	-37.36	0.0000	-4.6728	-4.2069
	/cut3	-1.8639	0.1085	-17.17	0.0000	-2.0766	-1.6512
	/cut4	0.9247	0.1065	8.68	0.0000	0.7159	1.1335
Iconcern_4	|						
	/cut1	-4.3918	0.0953	-46.07	0.0000	-4.5786	-4.2049
	/cut2	-2.7153	0.0870	-31.21	0.0000	-2.8858	-2.5448
	/cut3	-0.9870	0.0823	-11.99	0.0000	-1.1484	-0.8256
	/cut4	0.8297	0.0816	10.16	0.0000	0.6697	0.9897
Iconcern_5	|						
	/cut1	-3.4024	0.0793	-42.91	0.0000	-3.5578	-3.2470
	/cut2	-1.9986	0.0742	-26.95	0.0000	-2.1440	-1.8532
	/cut3	-0.4258	0.0714	-5.96	0.0000	-0.5658	-0.2859
	/cut4	1.1198	0.0719	15.57	0.0000	0.9788	1.2608
Isconcern_1	|						
	/cut1	-4.8865	0.0849	-57.56	0.0000	-5.0529	-4.7201
	/cut2	-1.8327	0.0617	-29.69	0.0000	-1.9536	-1.7117
	/cut3	0.9772	0.0594	16.46	0.0000	0.8609	1.0936
	/cut4	3.4212	0.0721	47.48	0.0000	3.2799	3.5624
Isconcern_2	|						
	/cut1	-6.0784	0.1264	-48.10	0.0000	-6.3261	-5.8307
	/cut2	-1.8396	0.0791	-23.25	0.0000	-1.9947	-1.6845
	/cut3	1.7172	0.0768	22.36	0.0000	1.5667	1.8677
	/cut4	4.6953	0.1028	45.68	0.0000	4.4938	4.8967
Isconcern_3	|						
	/cut1	-4.6780	0.0779	-60.09	0.0000	-4.8306	-4.5254

	/cut2	-1.4302	0.0556	-25.74	0.0000	-1.5391	-1.3213
	/cut3	1.6631	0.0570	29.20	0.0000	1.5515	1.7748
	/cut4	4.2245	0.0745	56.67	0.0000	4.0784	4.3707
Isconcern_4	|						
	/cut1	-3.3559	0.0455	-73.68	0.0000	-3.4452	-3.2666
	/cut2	-1.9343	0.0254	-76.21	0.0000	-1.9840	-1.8845
	/cut3	-0.4885	0.0179	-27.25	0.0000	-0.5236	-0.4534
	/cut4	0.8945	0.0191	46.93	0.0000	0.8571	0.9318
Isconcern_4	|						
	/cut1	-3.4006	0.0463	-73.41	0.0000	-3.4913	-3.3098
	/cut2	-2.0510	0.0272	-75.49	0.0000	-2.1042	-1.9977
	/cut3	-0.5552	0.0193	-28.81	0.0000	-0.5929	-0.5174
	/cut4	0.9766	0.0205	47.55	0.0000	0.9363	1.0168
Itech	|						
	/cut1	-2.2808	0.0325	-70.22	0.0000	-2.3444	-2.2171
	/cut2	-1.2326	0.0252	-49.01	0.0000	-1.2818	-1.1833
	/cut3	0.2491	0.0223	11.17	0.0000	0.2054	0.2928
	/cut4	1.6555	0.0273	60.70	0.0000	1.6021	1.7090
Igovern	|						
	/cut1	-3.7207	0.1028	-36.18	0.0000	-3.9223	-3.5191
	/cut2	-1.6948	0.0742	-22.83	0.0000	-1.8403	-1.5494
	/cut3	0.0016	0.0608	0.03	0.9790	-0.1176	0.1208
	/cut4	1.4374	0.0653	22.01	0.0000	1.3094	1.5654
Ivote	|						
	/cut1	-2.1149	0.0284	-74.52	0.0000	-2.1705	-2.0593
	/cut2	-1.0659	0.0215	-49.60	0.0000	-1.1081	-1.0238
	/cut3	-0.0660	0.0192	-3.44	0.0010	-0.1037	-0.0284
	/cut4	0.9504	0.0207	45.92	0.0000	0.9098	0.9910
Ibus	|						
	/cut1	-2.1871	0.0426	-51.32	0.0000	-2.2707	-2.1036
	/cut2	-0.6285	0.0359	-17.53	0.0000	-0.6988	-0.5583
	/cut3	1.5272	0.0383	39.89	0.0000	1.4522	1.6023
	/cut4	2.7326	0.0468	58.35	0.0000	2.6408	2.8244
		Variance and Covariance					
var(e.Concern)		13.8376	0.4389	31.53	0.0000	13.00	14.7250
var(e.SConcern)		7.3585	0.2478	29.70	0.0000	0.10	0.1815
var(e.Distrust)		0.1343	0.0206	6.51	0.0000	0.75	1.0015
cov(e.Concern,e.SConcern)		1.9749	0.1103	17.91	0.0000	1.7588	2.1911

cov(e.Concern,e.Distrust)	0.2504	0.0352	7.10	0.0000	0.1813	0.3194
cov(e.SConcern,e.Distrust)	0.4894	0.0457	10.70	0.0000	0.3997	0.5790
Correlation (e.Concern, e.Sconcern)	**0.196**					
Correlation (e.Concern, e.Distrust)	**0.184**					
Correlation (e.Sconcern, e.Distrust)	**0.492**					

Table C.3 Health Results

Number of Observations 18,920

Log-Likelihood -249968 12.429

		Coef.	Std.Err.	z	P>|z|	[95% CI]	
Variable		**Factor Loadings (Privacy concern while using health information device)**					
Iconcern_1	Personal information (your name, address, health conditions) accessed by non-medical personnel (e.g. police)	1					
Iconcern_2	Personal information (your name, address, health conditions) accessed by private companies (such as pharmaceutical and insurance companies)	1.4983	0.05	30.14	0	1.4008	1.5957
Iconcern_3	Misuse of personal information for harassment based on race, health status, sexual orientation, etc.	0.8216	0.015	54.1	0	0.7919	0.8514
Factor Loadings (Westin's Distrust)							
Itech	Q31_1 Distrust(constrained)	1					
Igovern	Q31_2 Distrust	5.8465	0.672	8.71	0	4.5303	7.1628
Ivote	Q31_3 Distrust	0.6103	0.104	5.87	0	0.4065	0.814
Ibus	Q31_4 Distrust	3.9596	0.526	7.52	0	2.928	4.9912
Factor Loadings (Concern for health personal information usage)							
Iuse_1	A system that stores health information (such as your blood group, allergies, health conditions) can be useful in providing higher-quality treatments	1					

Iuse_2	A system that stores health-related information (such as your blood group, allergies, and health conditions) can be useful in preventing health epidemics (e.g. H1N1/swine flu)	1.0026	0.05	20.01	0	0.9044	1.1007
Iuse_3	I am concerned that in a health emergency there could be an unacceptable delay due to the time spent in identifying the person needing help and their health conditions before the treatment begins	0.3589	0.012	29.75	0	0.3353	0.3826
Latent Variable (Privacy concern of the personal information stored on the health device)							
Concern							
male	Male	-0.1979	0.052	-3.8	0	-0.3001	-0.0958
hlong	Require long-term treatment	0.2289	0.058	3.97	0	0.1158	0.342
hiedu	University and above	0.1462	0.061	2.38	0.017	0.0259	0.2666
HHIncome	Household income	-0.0001	0	-7.4	0	-0.0002	-0.0001
HHIncNA	Didn't specify income	-0.1478	0.075	-1.97	0.049	-0.2951	-0.0004
Latent Variable (Distrust)							
Distrust							
age	Age	-0.001	0	-5.19	0	-0.0013	-0.0006
hlong	Require long-term treatment	0.0447	0.008	5.67	0	0.0292	0.0601
HHIncome	Household income	0	0	-3.9	0	0	0
HHIncNA	Didn't specify income	-0.0266	0.008	-3.22	0.001	-0.0427	-0.0104
Latent Variable (Perceived usefulness of the health device/system)							
PerUse							
male	Male	-0.0732	0.051	-1.45	0.148	-0.1724	0.0261
age	Age	0.0129	0.002	8.18	0	0.0098	0.016
hiedu	University and above	-0.3355	0.06	-5.61	0	-0.4527	-0.2184
HHIncome	Household income	-0.0002	0	-12.5	0	-0.0002	-0.0002
		Indicator Thresholds					
Iconcern_1							
	/cut1	-4.3431	0.077	-56.45	0	-4.494	-4.1923
	/cut2	-2.4026	0.063	-37.9	0	-2.5269	-2.2784
	/cut3	-0.3227	0.056	-5.8	0	-0.4317	-0.2137
	/cut4	1.97	0.058	33.87	0	1.856	2.084
Iconcern_2							
	/cut1	-7.328	0.171	-42.79	0	-7.6637	-6.9924
	/cut2	-4.6762	0.124	-37.61	0	-4.9199	-4.4325
	/cut3	-1.8181	0.087	-20.83	0	-1.9892	-1.647

	/cut4	1.4017	0.087	16.12	0	1.2313	1.5722
Iconcern_3							
	/cut1	-3.5445	0.059	-59.59	0	-3.6611	-3.4279
	/cut2	-2.1644	0.052	-41.82	0	-2.2658	-2.0629
	/cut3	-0.6534	0.047	-13.93	0	-0.7453	-0.5614
	/cut4	0.9797	0.047	21.01	0	0.8883	1.0711
Itech							
	/cut1	-2.3511	0.029	-82.29	0	-2.4071	-2.2951
	/cut2	-1.2923	0.021	-61.15	0	-1.3338	-1.2509
	/cut3	0.1743	0.018	9.8	0	0.1395	0.2092
	/cut4	1.4535	0.021	68.68	0	1.412	1.4949
Igovern							
	/cut1	-3.6456	0.129	-28.35	0	-3.8976	-3.3935
	/cut2	-1.7703	0.089	-19.98	0	-1.9439	-1.5967
	/cut3	-0.1481	0.058	-2.56	0.01	-0.2615	-0.0347
	/cut4	1.1659	0.054	21.5	0	1.0596	1.2722
Ivote							
	/cut1	-2.0314	0.025	-81.68	0	-2.0801	-1.9826
	/cut2	-1.0592	0.019	-54.6	0	-1.0972	-1.0212
	/cut3	-0.0936	0.017	-5.45	0	-0.1274	-0.0599
	/cut4	0.8802	0.018	49.28	0	0.8452	0.9152
Ibus							
	/cut1	-2.308	0.053	-43.46	0	-2.4121	-2.2039
	/cut2	-0.7157	0.039	-18.2	0	-0.7927	-0.6386
	/cut3	1.4547	0.043	33.47	0	1.3696	1.5399
	/cut4	2.6901	0.055	48.78	0	2.582	2.7982
Iuse_1							
	/cut1	-6.5975	0.164	-40.27	0	-6.9186	-6.2764
	/cut2	-4.9905	0.134	-37.29	0	-5.2528	-4.7282
	/cut3	-2.3586	0.098	-24.11	0	-2.5504	-2.1669
	/cut4	1.0441	0.089	11.68	0	0.869	1.2193
Iuse_2							
	/cut1	-5.6668	0.144	-39.49	0	-5.9481	-5.3856
	/cut2	-3.9283	0.118	-33.22	0	-4.1601	-3.6965
	/cut3	-1.3006	0.091	-14.32	0	-1.4786	-1.1227
	/cut4	1.7533	0.092	19	0	1.5724	1.9341
Iuse_3							
	/cut1	-3.5782	0.05	-71.52	0	-3.6762	-3.4801

/cut2	-2.1739	0.038	-56.47	0	-2.2494	-2.0985
/cut3	-0.4989	0.034	-14.65	0	-0.5657	-0.4322
/cut4	1.1409	0.035	32.46	0	1.072	1.2098
Iuse_4						
/cut1						
/cut2						
/cut3						
/cut4						
Iuse_5						
/cut1						
/cut2						
/cut3						
/cut4						
Iuse_6						
/cut1						
/cut2						
/cut3						
/cut4						
	Variance and Covariance					
var(e.Concern)	11.3385	0.355	31.98		10.6644	12.0551
var(e.Distrust)	0.0577	0.012	4.78		0.0383	0.0869
var(e.PerUse)	9.3843	0.532	17.63		8.397	10.4877
cov(e.Distrust,e.Concern)	0.1054	0.018	5.85	0	0.0701	0.1407
cov(e.PerUse,e.Concern)	0.9783	0.102	9.57	0	0.778	1.1787
cov(e.PerUse,e.Distrust)	-0.1793	0.021	-8.74	0	-0.2195	-0.1391
Correlation (e.Concern, e.Distrust)	**0.13**					
Correlation (e.Concern, e.PerUse)	**0.095**					
Correlation (e.Distrust, e.PerUse)	**-0.244**					