PRISE
privacy • security

Security Research

PASR

Preparatory Action on the enhancement of the European industrial potential in the field of Security Research

Grant Agreement no. 108600
Supporting activity acronym: PRISE

Activity full name:
Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies

Activity type: Supporting Activity

Annexes to D 5.8 Synthesis Report - Interview Meeting on Security Technology and Privacy

Start date of Activity: 1 February 2006 Duration: 28 month

Author(s):
Danish Board of Technology

Supporting Activity Co-ordinator
Johann Čas,
Institute of Technology Assessment, Austrian Academy of Sciences
Strohgasse 45, A-1030 Vienna, Austria
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

Partners

Institute of Technology Assessment, Vienna, Austria
Contact: Johann Čas
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

The Danish Board of Technology, Copenhagen, Denmark
Contact: Lars Klüver
LK@Tekno.dk
www.tekno.dk

The Norwegian Board of Technology, Oslo, Norway
Contact: Christine Hafskjold
christine.hafskjold@teknologiradet.no
www.teknologiradet.no

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, Germany
Contact: Marit Hansen
prise@datenschutzzentrum.de
www.datenschutzzentrum.de

Table of Contents **page**

Annex 1 Method Handbook

Introduction

1.1 Summary of the PRISE project

PRISE will promote a secure future for European citizens based on innovative security technologies and policies in line with privacy protection and human rights in general by:

- developing and testing a set of criteria and guidelines for privacy enhancing security research and technology development
- elaborating these criteria and guidelines with direct involvement of providers of security technologies, private and public users and implementers, institutions and bodies shaping policies and regulation as well as organisations representing potentially and actually conflicting interests
- transforming the results into privacy enhancing development and implementation scenarios of security technologies and measures
- testing these scenarios in a set of participatory technology assessment procedures in different European states allowing for a substantiated indication of public perception and citizens' preferences
- disseminating the results to actors relevant for the shaping of technologies and policies
- increasing competitiveness of European security industries by providing guidance for the provision of widely acceptable security technologies

PRISE will perform a study in support of security solutions with a particular emphasis on human behaviour and the perception of security and privacy. It will assist the European Union in shaping their forthcoming security programme in order to achieve active contributions for maintaining security of its citizens with due regard for fundamental rights and democratic accountability at EU and national level by developing sets of criteria for privacy enhancing security technologies. These sets of criteria will be applicable on different levels (research, development, implementation) and by different actors (research coordinators, industry, policy makers, public and private users).

The criteria will contribute directly to a tangible and demonstrable improvement in security as accepted and acceptable security technologies will be easier implemented, more widely used and confronted with less disaffirmation from the general public and from users of these technologies. Privacy enhancing or at least compliant security technologies will also increase competitiveness of European industries and can therefore contribute to security on a global level.

PRISE will tangibly contribute to improved security by overcoming problems of acceptance of new technologies when there is no sufficient level of security and privacy taken into consideration. An important example where these problems cause a lack of acceptance are e-

commerce services; acceptance problems can be also be observed in the field of RFID because of shortcomings in the field of privacy

PRISE will also be important for security research programme design by testing the use of well-established methods of participatory Technology Assessment for security technologies and services. The experiences made and knowledge gained in this process could be of high relevance and importance for research policy and the development of future Framework Programmes in general. PRISE will generate important inputs and guidelines for distinguished security culture in Europe. In addition PRISE will increase competitiveness of European industry as supplier of acceptable and hence widely accepted security technologies. PRISE also offers a unique approach in two respects: the combination of user and stakeholder involvement with participatory Technology Assessment methods and the implementation of elements of constructive Technology Assessment in the preparation of a research programme on security.

1.2 Introduction to the present manual

"Human factors" play a big role when shaping and applying security policies. As a part of the PRISE project, citizen participatory activities – each involving about 30 citizens – will be carried out in 5 European Union member states and in Norway. The purpose is to establish a combined quantitative and qualitative insight into public perceptions. The participatory activities will take places in the four countries of the PRISE partners and there is further intention to conduct activities via subcontractors in a South and an Eastern European Union member state.

Work package 5 of the PRISE project is the participatory activity, which will provide insight into the public perceptions and citizens' preferences based on the scenarios that are developed in work package 4. The purpose of work package 5 is to provide input for the further development of criteria for privacy enhancing technologies, which will take place in work package 6.

The participatory methodology for work-package 5 is "the interview meeting". The interview meeting includes a questionnaire and a subsequent group interview.

This manual describes the methodology of the interview meeting. It further describes what to do when carrying out an interview meeting – step by step.

1.2.1 Who is the manual for?

This manual is designed for the partners and subcontractors that will carry out the interview meetings in connection with the PRISE project. The manual helps define the division of work and each partner's responsibility, making it possible for partners to efficiently plan their work, taking into account the workload and making sure that personnel with the necessary qualifications is available. Besides this manual, PRISE partners and subcontractors will receive a one-day training course on the interview meeting method. The training course is described in chapter 4.

1.2.2 Overview of manual

Chapter 2 is a general description of the method combined with more specific descriptions of how it will be implemented in the PRISE project. Chapter 3 focuses on the people involved in the interview meeting and chapter 4 is a step-by-step guide on how to carry out the interview

meeting in the PRISE context, as well as a timeline for the whole process, including preparation.

The interview meeting

1.3 What is an interview meeting?

The interview meeting is a method to gain knowledge of what a group of people think and feel about complex technologies. It is not a representative method but it aims at including a diverse group of citizens who cover a broad spectrum of demographic criteria such as age, sex, education and occupation.

Using group interviews and a questionnaire, a group of about 30 people are asked at the interview meeting about their perceptions and preferences in relation to a technology, a technological development, challenge or problem. As a rule, interviewees do not possess any expert or professional knowledge about the technology under exploration. However, prior to and during the meeting, the participants are informed about the advantages and disadvantages of the technology so that they share a balanced and factual starting point. In the PRISE project, this information is based on the scenarios developed in WP4 and the dilemmas that these scenarios focus on.

The interview meeting method employs a combination of a questionnaire and group interviews. These two methods complement one another well; the questionnaire ensures that all the participants are heard and that there is comparable data relating to the most important areas. The group interview, on the other hand, creates a lively debate and ensures that the participants can include aspects that are not addressed by the questionnaire. Interview meetings are particularly suitable in cases where:

- There are complex issues (technically complex and/or ones posing dilemmas)
- Prior public knowledge is limited
- An ethical dimension is involved

The issues at stake in the PRISE project is security technology and privacy, and that makes the interview meeting a suitable method for involving citizens the PRISE project.

1.4 The purpose of the method

The purpose of the interview meeting is to gain insight into the various notions, wishes, concerns and attitudes prevalent among the interviewees. The interview meeting must provide an indication of the general views of the interviewees and the underlying reasons for these. The purpose is thus not to conduct an actual opinion poll. The interviewees' answers provide insight into:

- fundamental attitudes towards a given technology
- the underlying reasons for these attitudes
- the variety of arguments that exist among the interviewees
- how citizens weigh different arguments and ethical principles against one another

Within PRISE, focus is of course on security technology and how it can be developed and applied in a way that does not threaten privacy. The purpose of the interview meetings is to get citizens' feedback on the scenarios (developed in WP4) and the underlying dilemmas. The questionnaire and the interview guidelines combined with an analysis guideline will decide the more specific focus of the interview meetings. The development of the questionnaire, the interview guidelines and the analysis guideline is coordinated with the development of the scenarios.

1.5 Procedure description

The interview meetings are held in the respective national languages. Scenarios, questionnaire and interview guidelines must be translated from English to the respective national languages prior to the meeting – if necessary by a professional translator. After translation, the material must be reviewed by a security technology expert who can correct the technical terms that a translator may get wrong. The material should also be evaluated with reference to possible national or cultural differences.

1.5.1 Before the meeting

The interview meeting is held in the evening and takes the form of a three-hour after-work meeting. Two to three weeks before the interview meeting, introduction material in the form of the scenarios from WP4 (translated by organizers) is sent to the participants along with practical information about the interview meeting. The scenarios will give the participants an insight to security technology and privacy issues, as well as the dilemmas connected to the subject and what is for and against the different technologies.

In addition to the written material, the meeting begins with an introduction to the scenarios and dilemmas.

1.5.2 Expert presentations and time for questions

The interview meeting begins with an introduction. The introduction is presented by one or more experts in the field. Following this, participants can put clarifying questions to the presenters. Alternatively the presentation is given by the organizer, but questions from participants are still answered by the experts.

In the PRISE project it is important that the introductions and answering of participants questions are as similar as possible. The citizens should as far as possible get the same information in the 6 different countries.

The presentation will be done by a national experts on security technology and privacy issues or by the organizer. The expert/organizer will present the multiple aspects of the scenarios in an oral introduction. The oral introduction will be developed by DBT and translated to national languages (by the organizer). That insures that the introduction is the same in all the six interview meetings. After the introduction, the participants can ask questions to the expert. The answering of the participants' questions can differ from country to country and consequently the information to the citizens may differ. To avoid to many differences the national expert shall be introduced properly to the PRISE project, the scenarios as well as the concept of the interview meeting.

Present at every interview meeting will also be at least one member of the PRISE project (at as many interview meetings as possible the WP5 leader will be present). If the participants have

questions to the PRISE project, the PRISE member can answer the question with the organizer as interpreter.

Questions and answers shall be summed up by the organizer in the final report

1.5.3 Questionnaire

After the introduction, participants are handed the questionnaire. Participants have 30-45 minutes in which to complete the questionnaire. The questionnaire focuses on the same dilemmas as the scenarios. Questions can be put to the organizers or the experts throughout the session if necessary.

1.5.4 Group interviews

After the questionnaire, participants are divided into four groups of 6-9 people and group interviews are subsequently carried out. The group interviews focus on the same topics as those of the questionnaire. The group interviews are tape-recorded and follow an interview guide but smaller variations are allowed. The interviews are monitored by an interviewer whose task is to ensure that all of the participants are heard and that all themes and questions are discussed and answered. The group interviews last one hour.

1.6 Results

An interview meeting provides both quantitative and qualitative results. Questionnaire answers provide comparable, measurable, quantitative results and the group interviews are used to gather the more qualitative results that give nuance to those of the questionnaire. Comparison and analysis of the two sets of results offer a balanced indication of public attitudes towards a given technology. After the meeting the group interviews are transcribed and statistics on the questionnaires are prepared. In the final analysis the quantitative and the qualitative data is combined.

1.6.1 Indirect results

The interview meeting creates debate and participants gain new knowledge about – and often a new interest in – the topic. Participants often continue debating the issue with their acquaintances.

1.6.2 Handling the results in the PRISE project

In the PRISE project the results of the interview meetings will be analyzed by each partner/subcontractor on the basis of an analysis guideline so that the national results will be comparable. The reports shall offer an analysis of both the qualitative and quantitative results. The report shall also contain a transcript of the group interviews and a list of questionnaire responses. All reports and results shall be presented in English, except the transcript of the group interviews which does not have to be translated into English.

The results will basically give insight into the participating citizens' priorities and there evaluation of dilemmas connected to security technology and privacy. The citizens will give their unique input from their "citizen logic".

The six national reports will be compared in a synthesis report made by the WP5 leader and reviewed by the other five partners/subcontractors. The aim of the synthesis report is – as far as

possible – to compare the results of the six national interview meetings. The results and the synthesis report will also be discussed at a review meeting in September 2007 in Copenhagen.

Necessary qualifications

1.7 The various roles and necessary skills

1.7.1 WP 5 leader

As WP 5 leader the Danish Board of Technology (DBT) will support the organizers by the present manual. Besides that DBT will carry out a training course (more details in chapter 4). DBT will also:

- Develop interview guidelines and questionnaire
- Develop guideline for data processing and report
- Write experts introduction to participants at interview meeting
- Make a template for invitation, confirmation and refusal letter
- Write script for the oral introduction to the citizens at interview meetings (material based on the work of the PRISE project)
- Collect quantitative material from all interview meetings and run them through SPSS before sending the data back for analysing
- Write the synthesis report build on the national reports

1.7.2 Organizers

Each national partner/subcontractor will function as organizer in carrying out their national interview meetings. Overall this means responsibility for preparing and running a national interview meeting. This includes a number of tasks that is described further in the chapter 4. Basically it requires that the organizer:

- has experience in the planning and running of a workshop
- has experience in conducting qualitative group interviews and can engage four trained interviewers and one or two security/privacy experts
- has experience and academic qualifications in analyzing both qualitative and quantitative data
- is trained in English at scientific writing level

It also requires that partner/subcontractor is:

- An independent non-stakeholder
- An established organization

1.7.3 Interviewers

Four trained interviewers are present at the meeting to conduct group interviews. These interviewers must have experience in conducting qualitative group interviews.

The interviewers must also be informed about the method as well as the PRISE project at a face-to-face meeting with the organizer prior to the interview meeting.

1.7.4 Expert

A security/privacy expert shall be present at the interview meeting to do the introduction to the scenarios and answering questions from the participants. The expert should be balanced in relation to the subject and if that is not possible there shall be two experts – one from each side. The expert should also be informed about method as well as the PRISE project prior to the interview meeting, and the expert can also be used when evaluating the translation of the scenarios.

1.7.5 Participants and recruitment

The recruitment of citizens is an important aspect of the legitimacy of a participatory initiative. The process needs to be effective in terms of its consistency so that results are comparable, and it needs to be a transparent process so all participants are aware there are no vested interests being pursued. The process should also be effective with regards to cost and response rate.

About 30 people take part in an interview meeting. Participants at an interview meeting will never be a representative cross-section of society. However, as the aim of the interview meeting is to determine attitudes among the general population, selection should focus on those candidates offering the best possible representation (variation) in terms of age, gender and education. The selection should also take into consideration that there is a variation in employment and that participants have no special prior knowledge of the topic of the interview meeting (e.g. no experts on privacy or employers from security technology companies).

The participants are selected on the basis of the applications from invited citizens, and should as far as possible be based on the following matrix:

Selection matrix

	18-34 years			35-54 years			55 + years		
Men									
Women									
	l	m	h	l	m	h	l	m	h

L = low education (secondary school, leaving age 15/16)

M = medium (college or equivalent; leaving age 18)

H = higher education (university or equivalent)

It is important that there are at least 25 participants. There are almost always some registered participants that do not show up on the day of the interview meeting (normally app. 10 percent). To make sure that there is at least 25 participants the organizer must have at least 30 registered participants and at best 35.

Recruiting the citizens should be done by sending out an invitation letter to 2000 randomly selected citizens (addresses). The random selection of addresses is within the capital (or regional capital) centre and surroundings (meaning within up to the radius of approximately 100 km from the city hoisting the interview meeting).

The invitation shall be send out along with a short presentation of the project and the interview meeting, a reply form and a return envelope. The reply form ask for information about age, gender, education, employment and prior knowledge to the subject. There should be a relatively short answering deadline (e.g. two weeks).

If more than 35 citizens register, the participants will be selected on the basis of the matrix above.

If sending out 2000 invitations does not provide 35 registered participants, the organizer must proceed inviting citizens by selecting 100-200 random telephone numbers and calling citizens personally to make them interested.

If there is still not 35 registered participants, citizens can be invited by the co-nomination method, where invitation starts in the organizers own personal network and is spread out from here.

1.8 What to do – step by step

1.8.1 Participate in 1-day training workshop

The partners must participate in a 1-day training workshop that will take place on April 11th 2007 in Copenhagen. The participants in the training workshop will be the organizers who are going to carry out the interview meetings in the six countries. Interested team members can participate as well.

The training workshop will include:

- An introduction to the methodology
- A detailed description of all the tasks that have to be carried out in order to complete an interview meeting
- A time plan
- Discussion of the questionnaire and interview guideline
- A briefing on how to analyze and report from the meeting

1.8.2 Find location

At an early stage the organizer must find the location for the interview meeting. The location should offer one room (app. 50 persons) for the plenary sessions and 3-4 smaller rooms for conducting the group interviews. All rooms should be available from app. 2 hours before the meeting for preparation (testing recording equipment etc.) and until the end of the meeting. The location must also be easily accessible for participants, e.g. close to public transportation, and services such as food and beverages should be provided.

1.8.3 Translate all material into national language

All material (15-20 pages) is to be translated from English to the organizers national language. If necessary the partners must hire a professional translator. The material includes invitation template (and other letters), questionnaire, interview guidelines and scenarios.

1.8.4 Run a small pilot test of the questionnaire and the interview guideline

Before the interview meeting, partners must run a small pilot test to investigate whether the questionnaire and interview questions is understood or not. The partners report the results of the pilot test and possible need for changes back to the Danish Board of Technology.

1.8.5 Recruit citizens for national interview meeting

Each partner or subcontractor must recruit 35 participants according to the guidelines made by The Danish Board of Technology.

1.8.6 Arrange and carry out national interview meeting

Arranging and carrying out the interview meeting involves a number of organizing tasks, e.g. finding location, providing food and beverages, finding one or two persons who can introduce the scenarios, finding 4 interviewers, make sure the A/V equipment and other technique is in order.

As a separate task, organizers must hold an eye on public debate and the media to register if there is any security or privacy issues that might affect citizens attitudes at the meeting. This should be done the last two weeks prior to the interview meeting.

1.8.7 Complete the national data processing

After the interview meeting partners must complete the data processing. Data processing includes transcribing the group interviews, analyzing both the qualitative data from the group interviews and quantitative data from the questionnaire. The quantitative data from the questionnaire is sent to DBT, who will do the data processing using SPSS version 10.0 before sending it back to the organizers for further analysis. Analyzing of the data shall follow the analysis guideline made by The Danish Board of Technology.

1.8.8 Write the national report

Each partner describes the results in a national report that will be part of the synthesis report. National reports shall be 10-15 pages of analysis plus a transcript of the group interviews and a list of questionnaire responses. Specific criteria for the national reports will be a part of the analysis guidelines.

1.8.9 Review the synthesis report

The six national reports will be part of a synthesis report. All organizers must review the synthesis report. The partners and subcontractors must participate in a 1-day workshop in Copenhagen where reviews and comments on the synthesis report will be discussed.

1.9 Timetable

Time plan 2007	**Partners tasks**
April 16th - 20th	Find locations for interview meetings. Find people who can carry out and transcribe the group interviews. Find translators for the written material and the transcriptions
April 20th	Documents ready for translation: Invitation letter, confirmation letter and refusal letter
April 23rd – 29th	Start to recruit citizens. Find people who can do the oral introduction at the interview meeting
May 1st	Documents ready for translation: Interview guide, questionnaire
May 1st – 10th	Translate interview guide, questionnaire and introduction papers for citizens
May 10th - 15th	Carry out a pilot test and report back to DBT
May 16th	Documents ready translation: Expert presentation
May 16th	The last two weeks up to the interview meeting organizer holds an eye on public debate and the media to register if there is any security or privacy issues that might affect citizens attitudes at the meeting
May 18th	Deadline for recruiting citizens
May 21st	Send out introduction papers to citizens
June 1st	Documents ready for translation: Analysis guide (analysis questions and report format)
June 4th - 15th	Carry out national interview meetings
June – August 15th	Write national reports (including data processing, transcription of interviews and translation of interviews and reports
August 15th	Deliver national reports in English according to guidelines
September 11th	Review synthesis report at a 1-day workshop in Copenhagen

Annex 2 Composition of Participants

	18 – 34 years			35 – 54 years			55 + years		
Men	6	9	10	5	10	15	5	7	11
Women	2	9	6	7	10	15	4	16	11
Education	**S**	**M**	**H**	**S**	**M**	**H**	**S**	**M**	**H**

In the final selection of participants all countries, we find that although sex and age are distributed as intended, there are fewer participants with short educations.

Annex 3 Scenarios

Introduction

This document will present you with some scenarios showing how security technologies and surveillance may be used in everyday situations – in the near future.

What is security technology?

Security can be defined as the absence of danger – that is a state where the desired status quo is not threatened or disrupted in any way. In the context of the **PRISE** project, security is understood as the security of the society – or more precisely – of the citizens that constitute the society.

The term *security technology* can cover everything from private alarm systems and virus protection systems for PCs to border control systems and international police co-operation. In our scenarios we mainly focus on technologies or means (systems, legislation etc.) that are meant to enhance the security of the society against threats from individuals, or groups of individuals (not from states). This covers crime-fighting, anti-terror activities, border control activities etc.

In the scenario text we introduce some facts about the different technologies, to help you understand how they work today and their potential for the future.

What is privacy?

Privacy is generally associated with the protection of the integrity, autonomy and private life of the individual. Basically, it's about people's right to choose how they want to live their life, and what things they want to keep private. Privacy is considered a basic human right, and the first regulation of privacy is article 12 in the Universal Declaration of Human Rights.

What makes the protection of privacy difficult is the fact that privacy is almost always competing against other goods in society, such as mobility, efficiency, security or convenience. For example; even if we know that carrying a mobile phone that is turned on makes it possible to trace where we are, most of us would not dream of leaving the phone at home! And most people prefer having an RFID token in their car, rather than waiting in line to pay with (anonymous) cash when driving onto a toll-road.

Research suggests that many people are not concerned about technologies that infringe their privacy because they feel they have nothing to hide. Experts fear that this will result in a loss in privacy for the society that can be difficult to regain once it is gone. And even the most law-abiding citizen may find himself in a situation where he wouldn't want to be watched or traced.

When it comes to security technologies and surveillance, critics claim that a lot of the measures that are implemented are not suited to combat terror, but only to reassure the public that "something is being done". This is because the measures can be circumvented or because the threat they address is too unlikely to justify the action taken against it. A much used example of this is the banning of anonymous calling cards in many countries. Critics of this ban claim that it only stops ordinary people who would like to be anonymous; the criminals

have ways of circumventing it by registering with a fake identity or using stolen mobile phones.

Some of the anti-terror initiatives, in particular in the United States, are very privacy infringing, such as eavesdropping telephone calls, screening electronic communication without a warrant or analysing someone based on data collected from different sources without informing the person in question.

An important privacy principle is that a person should be informed when his or her personal data is stored and processed, and that it is possible to get access to the data and check that it is correct. Personal data should only be collected and stored if it is really necessary and it should be deleted when it is no longer needed for the original purpose.

How do you feel about security technologies? Scenarios to inspire discussion

In the following section we will present you with the stories of two people: Carla and Peter. We will follow them in their encounters with different security technologies and means, and share their thoughts and ideas on these issues. In order to make the scenarios general, we have avoided using specific countries, cities or airports as examples. Instead, we have tried to show how different countries – and security authorities – have chosen different approaches to implementing security technology. The scenarios are placed some time into the future, in order to show the use of some security technologies or legislation that are not adopted yet.

We hope that these stories will inspire you to reflect on security and privacy, and how you feel about these two values.

Carla is 62. She has worked as a teacher all her life, but she is now considering early retirement. Everything is getting so technical these days! And the children seem noisier than before. Maybe she is getting old? This week, however, she will not worry about that. It's the beginning of the summer holiday, and she is visiting her son in a neighbouring country.

Carla gets on the underground to go to the central train station. She has "charged" her *Universal ticket* and uses this to pay for her journey by holding it in front of the reader at the bar. The ticket is a plastic card that contains a small chip. The chip keeps track of how many journeys she has left in her card. Carla has chosen a so-called anonymous ticket. She knows this means that the money is lost should she loose her ticket, and its also a bit extra hassle as she has to have the separate card. The regular *universal ticket* is of course embedded into the holder's *mobile unit*. You just have to carry the unit on you or in your purse, and verify with your fingerprint when you pass the bar.

Carla can't help it, she finds using finger-printing to identify herself unpleasant. She notices, of course, that the young today don't seem bothered by it at all, but to her it will always be associated with criminals and arrests. "It's bad enough that you have to give up your fingerprint and show your ID card when you want to travel abroad", she thinks. She definitely does not want to do it more often than she has to!

Biometrics

Biometric technology identifies individuals automatically by using their biological or behavioural characteristics. Biometrics can be used to control access to physical locations or to information (computers, documents). The most commonly used biometrics are fingerprints and facial characteristics.

The process of comparing the biometric from a person against a previously stored template is called matching. The matching results in a score. If the person is accepted or rejected is then based on whether this score exceeds a given threshold.

In most cases, the biometric image is stored in the form of a *template*, which is a digital representation of the biometric. The template is created using an algorithm. For privacy reasons, it is recommended to only store the template, and discard the original image. However, in law-enforcement systems, like biometric passports, and facial recognition systems, the original image is often retained.

We can distinguish between *identification* which is finding out who a person is by comparing his or her sample to all the templates that are stored in a system, and *authentication*, where the sample person is compared to his or her stored template, in order to verify that the person is who he or she claims to be.

One challenge with biometric systems is finding the right balance between the False Acceptance Rate (FAR) and False Rejection Rate (FRR). *False acceptance* (or *false positive*) is when a system identifies an individual incorrectly. If the system fails to identify an individual that is registered, it is referred to as *false rejection* (or *false negative*).

One of the major advantages with biometrics is that they are so strongly linked to a person. Biometric authentication provides better access control, and identity theft becomes a lot more challenging when personal data are linked exclusively to the right person. But this is also the greatest liability of biometric systems. Once a set of biometric data has been compromised, it is compromised forever.

Peter is 32. He works as a sales representative for a car dealership. This morning he is getting up early to go to a car show in Central Europe.He gets up, takes a quick shower, grabs his bag, gets into his car and heads for the airport. He's late as usual, but as he has registered for the *fast lane*, he should be OK. The fast lane lets you skip all the hassle with check in where passengers are checked against profiles of criminals, passports are checked, and of course there's the rigorous security check. With the fast lane you go through a particularly thorough registration process once – and let the airport store all your data. In return, you can bypass ordinary check in, and just authenticate yourself using biometric technologies at the entrance.

He sends a thought to his colleague who, in Peter's mind, has a fixation on privacy. He claims there is too much surveillance in the society as it is, and now he won't even accept cookies to his computer! He even uninstalled the Google toolbar - nobody does that! If it were true that American agencies use those data to map networks and scan for suspicious profiles, surely that would be common knowledge? Right now he's probably been up a couple of hours, and is already standing in line for check in and security. Well – he asked for it! Peter just hopes his colleague will get through security in time for them to go over their presentation one last time before boarding.

- o -

Carla arrives at the central station. As in the underground, there are cameras everywhere. Screens and loudspeakers on the walls repeat security warnings till nobody notices them anymore. "– Don't leave your bags unattended." "– Your image will be checked against the database of known terrorists." There was a debate about that last one a few years ago. Many countries don't signpost that they capture images and check against different databases, and it was suggested that they shouldn't have to do it here either. But the government was very clear on the principle that people should know when and where they are being checked. "That's particularly important when you have no way of noticing it yourself. You can't really know anymore if your picture is taken", Carla reflects. She has heard that there are countries where they also screen people's e-mails and phone conversations for words and phrases that are suspicious – but surely that must only be rumours!.

Carla feels her head spin with all the noise and heads for the *silent zone*. She has to show her ID to get in, but once inside, she relaxes. "No cameras, no mobile phones, no wireless zone, no noisy warnings! There really should be more such technology-free zones", she thinks.

It's not that she's not used to the cameras. After all, they've been around for most of her adult life, but don't they seem more

intrusive lately? After they started using both facial and pattern recognition software she seems to feel more observed and evaluated than before: "Am I making a terrorist-like movement now?" Imagine how embarrassing it would be to do something that might cause her to be stopped and checked by the anti-terror police! To be fair, she has never actually been stopped, but she can't help thinking about it when there are cameras around.

And, like most people, she knows someone that has actually been suspected of being a terrorist. When the technology was in its early phase there were a lot of problems with the facial recognition software. And because the politicians didn't want the scandal of someone on the watch list actually fooling the system, the result was a lot of so called *false positives*.

A colleague of hers, whose parents are from Iran, got mistaken for a terrorist. He found it very humiliating, and she doesn't blame him. Like he said: "When you have been arrested by anti-terror police dressed in bullet-proof vests and you look like me, people look at you differently afterwards – even if you are let off with an apology". Carla knows that he stayed away from the most camera-dense areas for a while after that, especially when he had his children with him.

Lately more and more people have been questioning both the legitimacy and efficiency of the cameras. In some areas of the city they are now starting tests where instead of surveillance cameras they install better and brighter street lights. Apparently with good results!

- o -

Working at a car dealership, Peter always has the latest model car. The one he is driving right now has all the newest technology: Galileo satellite connection with navigation system, automatic emergency call through the eCall-system and a bunch of other Vehicle Safety Systems. Peter isn't even sure what all of them do. The eCall system is now standard in all new cars, and it is supposed to call the emergency number automatically if the car is in an accident. Because it is connected to the Galileo system, it has the exact position of the car.

Closed Circuit Television (CCTV)

CCTV surveillance with *active cameras* is when an operator watches the monitor and can control the camera (turn, zoom) to follow an individual or a situation that develops. Active cameras can be used with automated visual surveillance programs that use algorithms to detect suspicious motion or identify people by comparing their image to a reference in a database.

Passive cameras: These cameras record what happens in a specific spot (for instance in a kiosk) on a tape. The tape is viewed only if there is an incident, like a robbery, fight etc.

While the earlier CCTV systems were analogue, digital systems are becoming increasingly widespread. Digital image searching can save time in the locating of specific events or tracking crime suspects against an existing database, but it is a concern that such images also can be manipulated more easily.

Automatic face recognition

Automatic face recognition systems are systems where a person's image is captured automatically and compared to a database for identification or authentication. Identification of a random person based on this technique would require an extremely large database and processing capacity beyond what is feasible today. Such systems are therefore normally used to verify that a person is not on a list of for instance known criminals or terrorists.

Automatic Number Plate Recognition (ANPR)

ANPR systems read number plates picked up by CCTV and match them against a database. Systems for number plate recognition are in use in several countries. They are mostly related to toll booth passing or speed cameras, but they are also used to identify stolen vehicles.

Over the last years there have been suggestions to use the technology for other purposes as well. After an attempted terrorist attack in Berlin, the terrorists stole a car and fled through Germany. It then turned out that the system could also be used to track the car, and even stop it! It turned out that the car was an expensive model with the latest in anti-theft technology, and that it could actually be stopped remotely via satellite. The terrorists were stopped and arrested, and after this the EU member states agreed that the systems could also be used by the police for tracking criminals and suspected terrorists.

After a research report on how many lives could be saved in traffic if the speed limits were respected by motorists, it was suggested that the Vehicle Security Systems should integrate a module that could check the speed limit on a given stretch of road and match the speed limit against the speedometer. The original suggestion was that a chip in the engine should make sure that no car could drive above the speed limit, but this was met with heavy protesting, both from the car industry and the car-owners associations. At the moment, the system is set up so that every time a car drives above the speed limit, a call is made to the central fine registry, and the fine is automatically deducted from the car owner's bank account.

Peter pushes the accelerator. All road stretches have still not been updated in the system, and he has downloaded an overview of which it is to his navigation system. He gets an alert every time he passes a sign that is hooked up to the system – meaning that he "has to" keep within the speed limit. "It's good that surveillance can work the other way as well", he thinks.

Peter arrives at the airport. The licence plate of his car is already in the system, and his car is registered automatically as he drives into the car park. It's the same technology that is being used in the cities to identify stolen vehicles. He actually thought such a system would be superfluous after the eCall connected to Galileo was implemented, but apparently the more organised gangs know how to disable the system. And he knows that some countries even demand that the driver should be able to disable the eCall-system himself. Those kinds of requirements always make it more difficult for the car industry! And why is it that the criminals always seem to be one step ahead of the technology?

Locating technology

It is possible to calculate the approximate position of the user's mobile equipment by using known coordinates of for instance GSM base stations.

For more accurate positioning, satellite based systems are used:

GPS is short for *Global Positioning System*, a worldwide satellite navigational system formed by 24 satellites orbiting the earth. By using three satellites, GPS can calculate the longitude and latitude of the receiver based on where the three spheres intersect. By using four satellites, GPS can also determine altitude.

Galileo will be a global network of 30 satellites providing precise timing and location information to users on the ground and in the air. It is planned to be fully operational in 2010. It will be more accurate than the GPS system, and it will have greater penetration.

eCall

The eCall device contains sensors that are activated after an accident. It calls the emergency number and communicates information about the accident, including the time, precise location, direction and identification of the car.

The device will not be permanently connected to a mobile communications network, it will only connect after it has been triggered. There is however concern that this could change, about the transmitting of additional data (for instance for insurance companies), and about possible unauthorised access to databases where eCall data is stored. From September 2009, all new cars in the participating countries will be equipped with eCall.

Function creep

Database systems are vulnerable to so called function creep, that is the use of the data for something other that the original intention. An example of such function creep was seen when the Norwegian data base of asylum seekers – which also contains biometric information like fingerprints – was opened to the police in criminal investigations. The original intention of the data base was to help establish the identity of asylum-seekers.

He parks the car, gets out and heads for the terminal and the fast lane check-in entrance. He places his finger on the sensor and looks straight into the camera. A green light flashes and the door opens.

Even if the sensors are a lot better than they used to be, some people still have trouble using fingerprinting: His grand-father, for instance. Even though he is a very fit 80-year old, he is getting more isolated. You have to use your fingerprint with the ID everywhere these days, and he's uncomfortable with all the hassle that you have to go through when the sensor can't read your prints. So he stays at home mostly.

Peter sometimes goes to the library to borrow *real* books for him. It amuses him to think of what his library profile must look like. If it's ever analysed in search of suspicious individuals, the intelligence service might wonder why a man in his thirties borrows book like "Dating for seniors" and "Our friends the birds".

A few years ago, just after a major terrorist attack was prevented in the US, it was actually suggested that security agencies should be allowed to search all possible databases. And that was not only for suspected criminals or terrorist. They wanted to analyse all material in library databases, electricity and gas consumption patterns, traffic data for telephone and internet, travel data and shopping habits. By searching for suspicious patterns, they wanted to identify possible terrorists.

His colleague, Alex, had been outraged, and Peter had tried to argue with him: Surely they wouldn't be asking for this unless they had good reasons? Surely the authorities should do whatever they could to catch terrorists? Alex was not convinced, and had argued that at least they could do the analysis on anonymous data: "If they find something suspicious, they can get a court order to have the identity revealed. There's no legitimate reason why they should know everything about everybody!"

Peter hadn't really been much interested in debating the subject further, but his colleague had been on and on about it in every lunch break, and in the end he had signed a petition against the proposal. "But I don't really see the point", he said. "Surely this is only a problem for those with something to hide?" On the other hand, he caught himself wondering if it's been registered somewhere that he signed that petition…

Total Information Awareness (TIA)

Total Information Awareness (TIA) was a program with the US Defence Advanced Research Projects Agency (DARPA). The TIA program contained three categories of tools - language translation, data search and pattern recognition, and advanced collaborative and decision support tools.

The goal of TIA was to predict terrorist attacks before they happen. The system was intended to scan private and public databases, as well as the Internet, for transactions that might be associated with a terrorist attack. The US Congress stopped the funding of TIA in September 2003, but many of the programs within the system live on under different names.

Carla sits in the silent zone, reading her book for a while, and then heads for the security gate.

The security gate at the international train terminal came as a result of increased demand for control, not only in airports, but also other places where many people are congregated. She knows that in some countries there are even security checks at the entrances of shopping malls and sports arenas. A bomber was caught at a shopping mall near where her son lives a couple of years ago. Apparently they had just started using scanning equipment at the entrance, and the bomber didn't know. Even so, she is glad that it hasn't gone that far in her country. So far, only air and train terminals have security with passenger scanning.

She's not too worried about shopping malls herself – after all there haven't been any threats to her country as far as she knows. But she's seen statistics showing that more people are going back to shopping in the smaller shops in the town and city centres, and that the malls are claiming that they are loosing revenue because they aren't allowed to put up scanning equipment like *naked machines.*

Carla takes out her passport and walks up to the iris scanner. She knows that some countries still use fingerprints in their IDs and passports, but she feels that using iris is more secure. The reader compares her iris to the template stored in her passport. She used to be worried about that, but her son, who works in the IT industry, has assured her that it is completely safe now. "The original encryption in the first passport was quite weak", he said, "but with the encryption used now, a supercomputer would have to use thousands of years to break the encryption! And also; in the early passports, they stored the actual image of the face and fingerprints or iris. Now they only store a *template* – a digital representation of the most important feature of the iris and face. Even if some

Radio Frequency Identification (RFID)

RFID is a concept for automatic identification using radio waves. Tiny integrated circuits (tags) containing information are attached to documents or integrated in products. A *reader* can be used to read the information on the tags within range.

RFID tags come as both *active* and *passive* chips. Active tags - like tokens for toll booth passing - contain a battery and will therefore be bigger than passive tags, but they can contain more information and work over longer distances. Passive tags do not contain a battery, but get their energy from the radio signal from the reader. A typical application of passive tags is the new European passport.

Most tags will communicate with any reader, but there are also tags that require the reader to provide a password or some other credential.

Biometric passport

A biometric passport consists of the actual document, normally in the form of a booklet, and a tiny chip.

The chip contains mandatory and optional data In addition there is a photograph of the user as a visual link between the holder and the passport.

The International Civil Aviation Organization (ICAO) has chosen to use a chip that can be read at a distance (like an RFID tag). ICAO has chosen *face* as the primary biometric to be used in passports. *Finger* and *iris* are recommended as secondary biometrics. The EU has chosen to use only finger as the secondary biometric.

Biometric passports have raised much debate, in particular related to the security of the biometric information. It is feared that the information can be stolen by skimming (reading the information at a distance without the owner's knowledge) or eavesdropping (intercepting the information when it is transmitted).

To address these concerns a scheme for "basic access control" (BAC) has been developed. Under BAC the inspection system uses a "key" derived from numeric data elements in the Machine readable zone (the barcode) to "unlock" the chip so that the system can read it. BAC has been criticised for not being secure enough, and security experts have managed to break the encryption in only a short amount of time.

body should break the encryption, they would not be able to recreate the face or the iris to impersonate the passport holder."

She has also been reassured that the reader only stores her iris template long enough to compare it to the one on her card, and that it is not stored in a central database. She is not so sure what happens when her passport is checked at another border. Are the data deleted after the matching there as well?

She remembers there was a scandal a few years ago with a central fingerprint database – was it in the US? A lot of fingerprints were stolen by an employee and sold to international criminals. Thousands of people had their identity stolen and experienced all sorts of problems – from being "black listed" at borders to having their bank accounts emptied. It was particularly difficult because it took such a long time before the government actually would admit to loosing the data. And in the mean time nobody would believe that their identities were stolen – or indeed that it was possible to use somebody's fingerprints to steal their identity!

Carla knows better, though. Last summer a friend of her son's got his ID stolen, just before he and his family were going on vacation. He was afraid they would have to cancel everything because he would be "black listed", but apparently the Schengen information system that is used in many European countries registers people who have had their identity stolen. Because of this, he and his family could travel as planned, and he was never accused of being a criminal or a terrorist, although his ID was probably checked more thoroughly than the average traveller's.

After the ID check, Carla has to send her luggage through the scanner, before going through what used to be referred to as the *naked machine.* She is relieved that the actual naked machine never was bought for the airports and international train terminals in her homeland. The security authorities evaluated different machines, but decided that it was just as secure to have the kind of machine where items hidden under the clothing is projected onto a neutral image of a person.

Passenger scanning (*Naked machines*)

Technologies such as *backscatter X-rays or Terahertz radiation* has better penetration in materials than optics. This means that it can be used for detection and imaging of items concealed by clothing.

A "naked machine" utilises this type of technology to reveal if a person has weapons or explosives concealed on their body. There are different systems in use. Some reveal everything under the clothes – not just guns and explosives – hence the name. This type of airport security has been tested at Heathrow (Terminal 4) since 2004. Other applications take the images of concealed objects and project them onto a sexless mannequin.

Even at 62, Carla is self-conscious about her body, and she is glad the young men at the security gate does not get to see her naked. She needs to remove her shoes, but apart from that she experiences no problems and is soon seated comfortably on the train.

- o -

Peter crosses the airport hall over to Security. Of course – even the fast lane customers have to pass through some form of security, but they have their own gate, and they are all professional at this. No-one in *this* lane is wearing metal belt buckles, or is amateurish enough to leave loose change in their pockets. And it's been years since shoes made for the business segment contained metal. He sucks in his stomach and passes through the *naked machine*. "Why do they always have to keep such a low temperature in this room?" he thinks, and blushes as he notices that one of the security guards is a woman

Data retention

A database is defined as an organised collection of data. It is widely recognised that when different pieces of data about a person can be put together, it reveals more about that person than the information items viewed separately. An important privacy principle related to databases containing information about persons is therefore that only the data necessary to fulfil the purpose of the system should be collected, and that it should be deleted when it is no longer needed.

Lately, we have seen a trend where governments have wanted to store more data and connect database systems for purposes that are different from the original purpose, like security. The types of data most commonly referred to when data retention is discussed, is data related to ICT, such as communication data from phone, mobile phone and Internet traffic.

The EU has passed a directive on the retention of such data Data related to who is communicating, where and when will be stored, but not the content of the communication. The data can be stored for up to 2 years.

Various US departments reported in 2005 that they purchased personal information from so called *information resellers* for approximately $30 million. These businesses collect and aggregate personal information from multiple sources and make it available to their customers. The sources may be public records, publicly available information (for instance on the Internet) and information from proprietary sources such as private businesses.

roughly his own age. Even so, he is pleased that the airport uses the *real* naked machine. It just feels safer, somehow.

Peter notices an addition to the security that he hasn't seen before. After the naked machine there's a second "gate" that some of the passengers are asked to go through. He vaguely remembers hearing something about a new security feature being tested at this airport. It supposedly registers features like body heat, sweat, heart rate… Stuff that can be a sign of diseases like SARS or Avian flu, or indicate that a person is nervous. Some of the test subjects are escorted into interview rooms nearby. He's glad he wasn't singled out for the test, even if he is healthy and has a clear conscience. "But to put it up in the *fast track*? Don't they know the people who use that are busy?"

He heads to the gate and takes a seat. Maybe he should call Yasmin and let her know that he is coming? She works for the car manufacturer his dealership represents, and he met her at the last car show he attended. They hit it off right away, and he would really like to see her again. On the other hand he's reluctant to call her on his mobile. He knows that Yasmin's brother is very active in a youth group in his Mosque, and that Yasmin probably is on some kind of watch list as part of her brother's "network". He wishes he'd bought some anonymous calling cards the last time he was in Asia. It's no longer legal to sell such cards in Europe.

Eavesdropping

Different applications can be used for monitoring citizens and interaction between citizens, either over the internet, telephone network or in defined areas. One form of eavesdropping is often referred to as *wiretapping.* This is essentially to install a listening device in the path between two phones that are part of a conversation. Wiretapping can be set up on the suspect's telephone or on the telephones of persons he or she is expected to contact.

An extended version of wiretapping is to more indiscriminately tap all communication lines (phone, mobile, Internet) in search of conversations that may be of interest. An example of this is the Echelon network, which is run by an alliance between the USA, UK, Canada, Australia and New Zealand. The system was initially set up to monitor communication in or to the Soviet Union and Eastern Europe. Patterns of communication can be analysed, and content can be scanned for interesting keywords.

He doesn't want to use an internet service either. Who knows what the airport networks keeps logs of? He's not even sure how the rules are these days. Does the police have direct access to these kinds of

data, or do they need a warrant? He suddenly wishes that he'd paid better attention in the privacy debate. He'll definitely ask his colleague when he gets on the plane.

The last time he had dinner with Yasmin she mentioned that she was sure that her e-mail was being scanned, and she asked him to use an encryption program if he wanted to write to her. "An un-encrypted e-mail is like a postcard", she explained. "Anyone who gets access to it can read it – didn't you know that?"

He actually thought that he would write to her, but he discovered that the mail program they use at work does not have built-in encryption, and he never got around to installing another one. He hopes she is not mad at him for ignoring her all this time. "I'll explain it when we meet", he thinks.

It's time to board the plane. He approaches the gate, places his finger on the sensor and boards as one of the first passengers. There is still plenty of room for hand luggage. He sends a thought to his colleague who is probably still standing in line for the security check, before he leans back and closes his eyes.

- o -

"Mom's on her way," Carla's son says to his wife after having received a message on his mobile. "She should be here in three hours time". His mother doesn't know it, but the new mobile unit she got for Christmas is connected to a service called *Kid-watch*. The technology is a new version of the trackers you could see in old spy-movies, where surveillers could see their suspects as little dots on a map. The main difference is that by using the built in Galileo technology in the mobile unit, he can follow his mom's movements on a map even when he's sitting in his own living-room in another country.

He tries not to look at it much though – it feels a bit too much like prying into her private life, but he has put in some triggers that will sound alarms if she is immobile for a long time inside her house, or if she is not home at night. After all, she is getting older, and he can't look after her the way he feels he should when he's living in another country. His phone rings: "Hi, it's mom. I'm on my way now – should be at the station in about three hours"…

Privacy enhancing technologies

Technologies that contribute directly to preserve privacy are known as Privacy enhancing technologies (PETs).

Anonymisation is one such PET. There are services that can enable anonymous electronic communication for regular users. Such technology hides the connection between the user and the traces he or she leaves behind, and can therefore prevent unwanted identification. Traditional cash payment and unregistered (anonymous) calling cards are means that provide for anonymity.

Identity management is also a form of PET: In some cases you don't want to identify yourself, but use a pseudonym (for instance in forums on the internet). In order to make it more difficult to match data, it can be a good idea to have different user names (which do not reveal your identity) and passwords for different purposes. Identity management systems assist people in keeping track of their different user names. In some cases, the service in question may only need to verify a specific attribute – like age or credit limit. In such cases the *identity provider* (e.g. your bank, telecom provider or employer) can act as a trusted third party and guarantee that attribute, without revealing your identity.

Encryption is about distorting content to make it unreadable to others. Because all electronic communication is vulnerable to eavesdropping or manipulation, it is in many cases crucial that the communication is taking place on encrypted lines, or that the content being transmitted is encrypted.

Annex 4 Questionnaire and Interview Guide

4.1 Questionnaire

Questionnaire on Security technology and privacy

Welcome to the PRISE project questionnaire survey on the attitudes towards security technology and privacy

In this questionnaire you will be presented with a series of questions. *Please circle the number next to the answer you want to give.* You must give only *one* answer to each question, except when it is specifically said that "you can circle more than one answer to this question". If you circle a wrong answer, just cross it out, and circle the correct one. You are more than welcome to ask questions along the way if you have any doubts about the meaning of questions.

Background Questions:

1. Sex

1. Male
2. Female

2. Age *(open)*

- Age: ____

3. Number of persons in your household, yourself included?

1. 1 person
2. 2 persons
3. 3 persons
4. 4 persons or more

4. Do you have children?

1. Yes
2. No

5. Are there any children living at home? *(you can circle more than one answer to this question)*

1. No
2. Yes, 14 years of age or younger
3. Yes, more than 14 years old

6. What is your highest level of education?

1. Elementary School - 7 years of schooling
2. Intermediate School - 8 or 9 years of schooling
3. Vocational training (skilled level/craftsman's training)
4. Secondary school (high school graduation)
5. Short-term higher education (less than 3 years of study)
6. Medium length higher education (3 - 4 years of study)
7. Advanced higher education (more than 4 years of study)

7. Please state your occupation (*open text box)*

- Occupation: _____

8. Do you live in a city or in the country?

1. Metropolitan area
2. Provincial town
3. Rural district

9. How often do you use a mobile phone?

1. At least once a day daily
2. At least once a week
3. At least once a month
4. Less than once a month
5. I never use mobile phone

10. How often do you write emails?

1. At least once a day daily
2. At least once a week
3. At least once a month
4. Less than once a month
5. I never write emails

11. How often do you use the Internet?

1. At least once a day daily
2. At least once a week
3. At least once a month
4. Less than once a month
5. I never use the Internet

12. How often do you travel by public transport?

1. At least once a day daily
2. At least once a week
3. At least once a month
4. Less than once a month
5. I never travel by public transport

13. How often do you travel by airplane (One return trip counts as one time)?

1. More than 5 times a year
2. 3-5 times a year
3. 1-2 times a year
4. Less than 1 time a year
5. Never

14. How often do you travel by car?

1. At least once a day daily
2. At least once a week
3. At least once a month
4. Less than once a month
5. I never travel by public transport

General Questions about security technology and privacy

Below you will find a number of the statements about security technology and privacy that appear in the public debate. To which degree do you agree with these statements?

For each statement please indicate to which degree you agree

- If you believe that the statement is completely right, circle 1 "Completely agree"
- If you believe that the statement is right, but have some reservations, circle 2 "Partly agree"
- If you find it impossible to assess whether the statement is right or wrong, circle 3 "Neither agree nor disagree"
- If you believe that the statement is wrong, but have some reservations, circle 4 "Partly disagree"
- If you believe that the statement is completely wrong, circle 5 "Completely disagree"

15. "The security of society is absolutely dependent on the development and use of new security technologies"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

16. "Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

17. "If you have nothing to hide you don't have to worry about security technologies that infringe your privacy"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

18. "When security technology is available, we might just as well make use of it"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

19. "Privacy should not be violated without reasonable suspicion of criminal intent"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

20. "It is uncomfortable to be under surveillance, even though you have no criminal intent"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

21. "New security technologies are likely to be abused by governmental agencies"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

22. "New security technologies are likely to be abused by criminals"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

Security technologies

In this section you will be asked about your attitude towards specific security technologies and their use. The grey text boxes give very short pieces of information about the technologies that are questioned subsequently. The boxes contain some of the same information about technologies as the boxes in the scenarios send out before hand. For further information about the technologies see the scenarios.

One part of these technology questions focuses on acceptable use of the technologies and to these questions it will mostly be possible to give more than one answer.

The other part of the technology questions is specific statements. For each statement please indicate to which degree you agree.

Biometrics

Biometric technology identifies individuals automatically by using their biological or behavioural characteristics. Biometrics can be used to control access to physical locations or to information (computers, documents). The most commonly used biometrics are fingerprints and facial characteristics.

Biometric image can be stored as the original image or in the form of a *template*, which is a digital representation of the biometric. For privacy reasons, it is recommended to only store the template, and discard the original image. However, in law-enforcement systems, like biometric passports, and facial recognition systems, the original image is often retained.

One of the major advantages with biometrics is that they are so strongly linked to a person. Biometric authentication provides better access control, and identity theft becomes a lot more challenging when personal data are linked exclusively to the right person. But this is also the greatest liability of biometric systems. Once a set of biometric data has been compromised, it is compromised forever.

Biometric passport

A biometric passport consists of the actual document with an embedded chip containing biometric data. The chip can be read by a reader at a distance.

Biometric passports have caused debate, because it is feared that the biometric information on the chip can be stolen by skimming (reading the information at a distance without the owner's knowledge) or by eavesdropping.

One challenge with biometric systems is finding the right balance between the False Acceptance Rate (FAR) and False Rejection Rate (FRR). *False acceptance* (or *false positive*) is when a system identifies an individual incorrectly. If the system fails to identify an individual that is registered, it is referred to as *false rejection* (or *false negative*).

23. What biometrics would you be comfortable using for access control? *(you can circle more than one answer to this question)*

1. Facial characteristics
2. Fingerprints
3. Iris recognition
4. I will not be comfortable using any biometrics for access control
5. Don't know

24. Where is using biometrics for access control acceptable? ***(you can circle more than one answer to this question)***

1. Acceptable for security control in banks
2. Acceptable for airport security
3. Acceptable for security control in stores
4. Acceptable for border control
5. Acceptable for security control in central bus and train stations
6. Acceptable for security control in sport-stadium and other crowded places/events
7. Acceptable for security control in other private services not mentioned
8. It is never acceptable
9. Don't know

Specific statements about biometrics

25. "Storing biometric data (e.g. fingerprints or DNA samples) of all citizens in a central database is an acceptable step to fight crime"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

26. "The use of the biometric passport makes me feel insecure because of the risk of my biometric data being stolen"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

Closed Circuit Television (CCTV)

CCTV surveillance with *active cameras* is when an operator watches the monitor and can control the camera (turn, zoom) to follow an individual or a situation that develops. Active cameras can be used with automated visual surveillance programs that use algorithms to detect suspicious motion or identify people by comparing their image to a reference in a database.

Passive cameras: These cameras record what happens in a specific spot (for instance in a kiosk) on a tape. The tape is viewed only if there is an incident, like a robbery, fight etc.

Automatic face recognition

Automatic face recognition systems are systems where a person's image is captured automatically and compared to a database for identification or authentication. Such systems are normally used to verify that a person is not on a list of for instance known criminals or terrorists.

Automatic Number Plate Recognition (ANPR)

ANPR systems read number plates picked up by CCTV and match them against a database. Systems for number plate recognition are in use in several countries. They are mostly related to toll booth passing or speed cameras, but they are also used to identify stolen vehicles.

Passenger scanning (*Naked machines*)

Technologies such as *backscatter X-rays or Terahertz radiation* have better penetration in materials than optics. This means that it can be used for detection and imaging of items concealed by clothing.

A "naked machine" utilises this type of technology to reveal if a person has weapons or explosives hidden on their body. There are different systems in use. Some reveal everything under the clothes – not just guns and explosives – hence the name. This type of airport security has been tested at Heathrow (Terminal 4) since 2004. Other applications take the images of concealed objects and project them onto a sexless mannequin.

27. Where can you accept CCTV surveillance? ***(you can circle more than one answer to this question)***

1. In stores
2. In dressing rooms to prevent shoplifting
3. In central bus and train stations
4. In banks
5. In airports
6. In sport-stadium and other crowded places/events
7. In all public spaces
8. It is never acceptable
9. Don't know

28. How do you feel about the number of CCTV cameras in public spaces in general?

1. There should be more CCTV cameras in public spaces
2. The number of CCTV cameras in public spaces is appropriate
3. There should be less CCTV cameras in public spaces
4. There should be no CCTV cameras in public spaces at all
5. Don't know

29. Where is scanning of persons for detection of hidden items necessary for security reasons? *(you can circle more than one answer to this question)*

1. I schools
2. In central bus and train stations
3. In airports
4. In shopping malls
5. In public buildings (e.g. court)
6. It is never necessary
7. Don't know

30. What type of scanning would you find acceptable? *(you can circle more than one answer to this question)*

1. Scanning that reveal everything under the clothes
2. Scanning where images and hidden objectives are projected onto a mannequin
3. Scanning of body heat, sweat and heart rate
4. Scanning for metal objectives
5. Scanning luggage by x-ray
6. Scanning is not acceptable
7. Don't know

Specific statements about CCTV and passenger scanning

31. “CCTV surveillance makes me feel more secure”

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

32. “CCTV surveillance infringes my privacy”

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

33. “Scanning of persons for detection of hidden items is an acceptable tool for preventing terror”

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

Locating technology

It is possible to calculate the approximate position of the user's mobile equipment by using known coordinates of for instance GSM base stations.

For more accurate positioning, satellite based systems are used:

GPS is short for *Global Positioning System*, which is the existing system. *Galileo* is planned to be fully operational in 2010. It will be more accurate than the GPS system, and it will have greater penetration.

eCall

The eCall device contains sensors that are activated after an accident. It calls the emergency number and communicates information about the accident, including the time, precise location, direction and identification of the car.

The device will not be permanently connected to a mobile communications network, it will only connect after it has been triggered. There is, however, concern that this could change, about the transmitting of additional data (for instance for insurance companies), and about possible unauthorised access to databases where eCall data is stored. From September 2009, all new cars in the participating countries will be equipped with eCall.

34. For what purpose is locating of mobile phones acceptable? *(you can circle more than one answer to this question)*

1. Police locating mobile phones of suspected terrorists and criminals based on a court order
2. Police locating any mobile phone without a court order
3. In case of emergency, e.g. an accident, lost child or disoriented person
4. It is never acceptable
5. Don't know

35. For what purpose is locating of cars acceptable? *(you can circle more than one answer to this question)*

1. Police locating cars of suspected terrorists and criminals based on a court order
2. Police locating any cars without a court order
3. Police locating stolen vehicles
4. Speeding control and giving speeding tickets
5. Automatic locating and calling of the emergency number in case of a car accident
6. It is never acceptable
7. Don't know

36. Should eCall automatically be installed in all new cars?

1. Yes
2. Yes, but it should be possible to deactivate eCall
3. No, it should be optional
4. No, it should never be installed
5. Don't know

Specific statements about locating technologies

37. "The possibility of locating all mobile phones is privacy infringing"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

38. "The possibility of locating a suspect's mobile phones is a good tool for the police in investigating and preventing terror and crime"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

39. "The possibility of locating all cars is privacy infringing"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

40. "The possibility of locating all cars is a good tool for the police in investigating and preventing terror and crime"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

Data retention

A database is defined as an organised collection of data. It is widely recognised that when different pieces of data about a person can be put together, it reveals more about that person than the information items viewed separately. An important privacy principle related to databases containing information about persons is therefore that only the data necessary to fulfil the purpose of the system should be collected, and that it should be deleted when it is no longer needed.

Lately, we have seen a trend where governments have wanted to store more data and connect database systems for purposes that are different from the original purpose, like security. The types of data most commonly referred to when data retention is discussed, is data related to ICT, such as communication data from phone, mobile phone and Internet traffic.

Total Information Awareness (TIA)

Total Information Awareness (TIA) was a program with the US Defence Advanced Research Projects Agency (DARPA). The TIA program contained three categories of tools - language translation, data search and pattern recognition, and advanced collaborative and decision support tools.

The goal of TIA was to predict terrorist attacks before they happen. The system was intended to scan private and public databases, as well as the Internet, for transactions that might be associated with a terrorist attack. The US Congress stopped the funding of TIA in September 2003, but many of the programs within the system live on under different names.

Function creep

Database systems are vulnerable to so called function creep, that is the use of the data for something other that the original intention. An example of such function creep was seen when the Norwegian data

base of asylum seekers – which also contains biometric information like fingerprints – was opened to the police in criminal investigations. The original intention of the data base was to help establish the identity of asylum-seekers.

41. For which of the following purposes do you find data retention of communication traffic data acceptable? *(you can circle more than one answer to this question)*

1. For prevention of terrorist attacks in general
2. For investigation of specific terrorist attacks that have occurred
3. For prevention of crime in general
4. For investigation of specific crimes that have occurred
5. For commercial purposes
6. It is never acceptable
7. Don't know

42. For which of the following purposes do you find scanning and combining personal data from different databases acceptable? *(you can circle more than one answer to this question)*

1. For prevention of terrorist attacks in general
2. For investigation of specific terrorist attacks that have occurred
3. For prevention of crime in general
4. For investigation of specific crimes that have occurred
5. For commercial purposes
6. It is never acceptable
7. Don't know

Specific statements about data retention

43. "Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

44. "Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

45. "Scanning of and combining data from different databases containing personal information is privacy infringing"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

46. "Scanning of and combining data from different databases is a good tool for police to prevent terror"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

47. "Databases being used for something else than the original purpose is a serious privacy problem"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

Eavesdropping

Different applications can be used for monitoring citizens and interaction between citizens, either over the internet, telephone network or in defined areas. One form of eavesdropping is often referred to as *wiretapping.* This is essentially to install a listening device in the path between two phones that are part of a conversation. Wiretapping can be set up on the suspect's telephone or on the telephones of persons he or she is expected to contact.

An extended version of wiretapping is to more indiscriminately tap all communication lines (phone, mobile, Internet) in search of conversations that may be of interest.

48. For which of the following purposes is eavesdropping acceptable? ***(you can circle more than one answer to this question)***

1. For prevention and investigation of terrorist attacks *with* a court order
2. For prevention and investigation of terrorist attacks *without* a court order
3. For prevention and investigation of crime *with* a court order
4. For prevention and investigation of crime *without* a court order
5. For commercial purposes
6. It is never acceptable
7. Don't know

49. What methods of eavesdropping is acceptable?

1. Police eavesdropping all communication lines in search of conversation that may be of interest
2. Police eavesdropping lines of persons that suspect's is expected to contact
3. Police eavesdropping lines of suspects
4. Eavesdropping is totally unacceptable
5. Don't know

Specific statements about eavesdropping

50. "Eavesdropping is a good tool for police investigation"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

51. "Eavesdropping is a serious violation of privacy"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

Privacy enhancing technologies

Technologies that contribute directly to preserving privacy are known as Privacy enhancing technologies (PETs).

Anonymisation is one such PET. There are services that can enable anonymous electronic communication for regular users. Such technology hides the connection between the user and the traces he or she leaves behind, and can therefore prevent unwanted identification

Identity management is also a form of PET: In some cases you don't want to identify yourself, but use a pseudonym (for instance in forums on the internet). In order to make it more difficult to match data, it can be a good idea to have different user names (which do not reveal your identity) and passwords for different purposes. Identity management systems assist people in keeping track of their different user names

Encryption is about distorting content to make it illegible to others. Because all electronic communication is vulnerable to eavesdropping or manipulation, it is in many cases crucial that the communication is taking place on encrypted lines, or that the content being transmitted is encrypted.

52. What kinds of privacy enhancing technologies should be legally available for all citizens? *(you can circle more than one answer to this question)*

1. Anonymous calling cards
2. Encryption programmes
3. Identity management
4. No privacy enhancing technologies should be legal and available
5. Don't know

Specific statements about privacy enhancing technologies

53. "Privacy enhancing technologies are a necessity in today's society to preserve privacy"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

54. "Privacy enhancing technologies should not be legal if they make police investigation and prevention of terror and crime more difficult"

1. Completely agree
2. Partly agree
3. Neither agree nor disagree
4. Partly disagree
5. Completely disagree

Dilemmas in the use of security technology

We will now present you with a number of specific dilemmas in the use of security technology in proportion to the privacy consequences. For each dilemma we would like you to think about advantages as well as disadvantages and then answer the question. *You can give more than one answer to all of the questions in this section.*

55. Using your fingerprints in the underground to register when and where you are travelling could make it possible to automatically deduct the payment from your account. This would make payment a lot easier, but includes registration of your travelling and using your fingerprint for authentication. How would you feel about that? *(you can circle more than one answer to this question)*

1. I can accept registration of my travelling and using my fingerprints in the underground because it makes payment easier
2. I can only accept it if my fingerprints are stored only as a template and cannot be reconstructed
3. I can only accept it if the registration of my travelling is deleted after payment
4. Using fingerprints should be a possibility, but not the only form of payment
5. I would never use my fingerprints as identification in the underground
6. Don't know

56. Thorough registration in an airport database and acceptance of certain security technologies that can be regarded as privacy infringing, can make fast check-in at the airport possible. What security technologies and privacy infringements would you accept for faster check-in at the airport? *(you can circle more than one answer to this question)*

1. I would accept being thoroughly checked and registered in a permanent airport security database and then using biometrics for authentication on all further occasions
2. I would accept going through the "naked machine"
3. I would accept being scanned for sweat, body heat and heart rate
4. I would not give up privacy for fast and convenient check in at the airport
5. Don't know

57. Active CCTV surveillance cameras and automatic face recognition where faces of people are checked against a database of known terrorist are security technologies that can be used to prevent terror attacks, e.g. in airports or train stations. These security technologies could possibly prevent a terror attack, but the effect is not proven. They could also lead to innocent persons being mistaken for terrorists and taken aside for questioning. At what cost should these technologies be put to use? *(you can circle more than one answer to this question)*

1. Active cameras and automatic face recognition should be used no matter how many innocent persons are mistaken for terrorists

2. Active cameras and automatic face recognition should be used but only with a low rate of people mistaken for terrorists

3. Active cameras and automatic face recognition should only be put to use if no one is mistaken for terrorist

4. Active cameras and automatic face recognition should only be used in places where many crimes have occurred or that are very vulnerable to terror

5. Active cameras and automatic face recognition should not be used anywhere

6. Don't know

58. New technology makes it possible to scan and combine data from different databases containing personal information with the purpose of detecting suspicious patterns in personal communication and Internet use. The purpose is to foresee and prevent terror attacks, but it means scanning personal data from innocent persons. What police access to search and combine different databases do you find acceptable? *(you can circle more than one answer to this question)*

1. Police should have access to search and combine all databases for suspicious patters that can identify possible terrorists

2. Police should only have access to search and combine databases if the data is anonymous and only a court order can have the identity revealed

3. Police should never be allowed to search and combine databases for suspicious patterns

4. Don't know

59. The technology eCall could be installed in all new cars in order to call an emergency number in case of an accident. The eCall technology could also be used to locate cars for other purposes, e.g. if they are stolen or if they are used for crime or terror, but this requires that the movement of cars with eCall is registered at all times. What use of eCall do you find acceptable? *(you can circle more than one answer to this question)*

1. I find it acceptable that eCall can be activated by the police to locate a car if necessary to prevent crime or terror
2. I find it acceptable that eCall is active at all times and can be used to give speeding tickets
3. I find it acceptable that the movements of my car is registered at all times
4. eCall should not be used for any other purposes than reporting accidents
5. Installing of eCall in cars should be voluntary
6. Don't know

60. Privacy enhancing technologies (PETs) can contribute directly to preserving privacy when communicating by phone or mail and when using the Internet. But PETs can also be used for criminal activities and by terrorists. If the purpose is to preserve ordinary peoples privacy, what risks are you willing to accept for legal access to use of PETs? *(you can circle more than one answer to this question)*

1. I can accept legal anonymous calling cards, even though it might make police investigation and prevention of terror and crime more difficult
2. I can accept legal use of encryption, even though it might make police investigation and prevention of terror and crime more difficult
3. I can accept Internet anonymity, even if it means that persons searching for bomb instructions can not be traced by police
4. I can accept that Internet anonymity means that persons searching for child pornography can not be traced by the police
5. I can not accept any PETs that might make police investigation and prevention of terror and crime more difficult
6. Don't know

61. If a security technology provides high security, what consequences can you accept for people who are not able to use the technology and for people who refuse to use the technology for privacy reasons? *(you can circle more than one answer to this question)*

1. I can accept that people who refuse to use the technology for privacy reasons are excluded from using some public services
2. I can accept that people who are unable to use the technology are excluded from using some public services
3. I can accept that people who refuse to use the technology for privacy reasons are in some ways impeded when travelling by public transport
4. I can accept that people who are unable to use the technology are in some ways impeded when travelling by public transport
5. I can not accept any consequences for people who refuse to use the technology for privacy reasons
6. I can not accept any consequences for people who are unable to use the technology
7. Don't know

Democratic issues

In the following section you will be presented to some statements about democratic issues concerning new security technologies. Who should be allowed to exert an influence in the matter of security technology and privacy and how?

To which extent do you agree or disagree in the following views – please indicate your opinion of each point of view. Please give only one answer to each question.

62. "Politicians must always submit important questions to public debate and public hearings before making decisions on implementing new security technologies"

1. I completely agree
2. I partly agree
3. I neither agree or disagree
4. I partly disagree
5. I disagree

63. "The subject of security and privacy is so complicated that it makes no sense to include the general public in discussions of this issue"

1. I completely agree
2. I partly agree
3. I neither agree or disagree
4. I partly disagree
5. I disagree

64. "Human rights organisations are always entitled to be heard when important decisions on security and privacy are made"

1. I completely agree
2. I partly agree
3. I neither agree or disagree
4. I partly disagree
5. I disagree

65. "It is important that private companies involved in producing security technologies are also entitled to be heard when important decisions on security and privacy are made"

1. I completely agree
2. I partly agree
3. I neither agree or disagree
4. I partly disagree
5. I disagree

66. "In relation to significant decisions on the use of security technologies, it is imperative that alternative solutions are elucidated and included in the debate"

1. I completely agree
2. I partly agree
3. I neither agree or disagree
4. I partly disagree
5. I disagree

Proposals for privacy enhancing use of security technologies

In the following section we would like you to consider some possible proposals on how to implement, use and research in security technologies without infringing privacy. For every proposal we ask you to state the importance of carrying out the proposal.

- If you find it very important that the proposal is followed, circle 1 "Of high importance"
- If you find it important, but not top priority, you circle 2 "Of some importance"
- If you find that it is not very important, circle 3 "Of little importance"
- If you find that it is not important at all or the proposal should not be followed, circle 4 "Not important at all"
- If you are not sure what to answer, circle 5 "Don't know"

Proposals

67. Collection of personal data from unsuspicious individuals must be anonymous until identification is authorized by court order

1. Of high importance
2. Of some importance
3. Of little importance
4. Not important at all
5. Don't know

68. Only authorized personnel can have access to collected personal data

1. Of high importance
2. Of some importance
3. Of little importance
4. Not important at all
5. Don't know

69. Prior to implementing, new security technologies must be checked for privacy impact

1. Of high importance
2. Of some importance
3. Of little importance
4. Not important at all
5. Don't know

70. Funding of research projects on new security technologies should be dependent on a thorough analysis of privacy impacts

1. Of high importance
2. Of some importance
3. Of little importance
4. Not important at all
5. Don't know

Final Questions

You have answered many diverse and detailed questions about security technologies and privacy. In conclusion we would like to ask you two final questions.

71. Have you changed your attitude towards security technologies in general in the course of completing this questionnaire?

1. Yes, my attitude towards security technologies in general has become more positive
2. Yes, my attitude towards security technologies in general has become more worried
3. No, I have not changed my attitude
4. Don't know

72. If there are any comments concerning security technologies that you would like to add or that you have not had the opportunity to express in this questionnaire, please feel free to make a remark below: *(open text box)*

1. I have nothing to add
2. Your remarks

_____
_____
_____
_____
_____

4.2 Interview Guide

Questions in bold must be discussed by the participants. Subsequent to every question is a short note on the purpose of the question. To most of the questions there is some subordinated questions. These subordinated questions are inspirational, and can be used to support the discussion if necessary. The subordinated questions does not have to be raised if it is not necessary to inspire the debate.

Interview questions

1. **What are your immediate thoughts about security technologies and privacy?**
   Purpose of the question: An open question to get the debate started and to give the participants the chance to present their immediate attitudes

2. **What do you think about the scenarios?**
   Purpose of the question: Make the participants talk about what they have read in the scenarios to get an idea of how their feel about the possible future presented within them

   Subordinated questions to inspire the debate – only if necessary:
   - How is the balance between security and privacy in the scenarios?
   - Do you think the benefits in the scenarios are important to achieve?
   - Do the scenarios draw a picture of an attractive future?

3. **What do you think are the important positive potentials of security technologies?**
   Purpose of the question: Make the participants focus on the positive potentials and get an impression of what they find is the most important gain of security technologies

   Subordinated questions to inspire the debate – only if necessary:
   - What can you gain with security technologies – try to give some examples?
   - What is the most important positive possibility?
   - Why is it important?

4. **What negative effects of security technologies are you worried about?**
   Purpose of the question: Make the participants focus on the negative side of security technologies, the threats, and get an impression of what they find is the biggest threat

   Subordinated questions to inspire the debate – only if necessary:
   - What are the negative effects of security technologies – try to give examples?
   - What is the most important negative effect of security technologies?
   - Why is it important

5. **When do you think security is more important than privacy – and opposite?**
   Purpose of the question: Make the participants debate the dilemma of security and privacy (the trade off) to get an impression of in which situations and how much

privacy they will give up for security

Subordinated questions to inspire the debate – only if necessary:
- In which areas or situations do you find that it is okay for security technology to infringe privacy?
- In which areas or situations do you find that privacy is more important than security?

6. **Who should be involved when deciding on implementing new security technologies?**
Purpose of the question: To get the participants input on the democratic perspective and importance of involving different interest groups when deciding on implementing new security technologies

Subordinated questions to inspire the debate – only if necessary:
- Which interest groups should be heard? (Citizens in general, civil rights organizations, security technology developers, politicians etc.)

7. **Do you have any suggestions about the regulation of development and implementation of new security technologies?**
Purpose of the question: To get the participants input on how to manage development and implementation of new security technologies

Subordinated questions to inspire the debate – only if necessary:
- Should there be any limitations on development of security technologies or should security technology companies develop anything they like?
- Should governments implement every security technology they find important or should there be some regulations – and what regulations?

8. **Has your participation in today's event changed your attitude towards security technologies and privacy? If so: Why?**
Purpose of the question: To find out if information and debate about security technologies and privacy have changed the participants attitudes toward the subject

9. Do you have any final remarks, points or messages that you would like to ad? (take a round)
Purpose of the question: To give the participants a change to make a last statement before ending the interview meeting

Subordinated questions to inspire the debate –only if necessary:
- Have something made a special impression on you during the conversation?

Rules of thumb

"Rules of thumb" and tips on how to carry out the group interview in a good way.

Introduction

Start by presenting yourself, "My name is … I'm from …, and I'm going to be the moderator at this group conversation. But you just talk and I will make a list of speakers if necessary.

After that you do a presentation round where people say their name and why they have come to the interview meeting

After that the TAPE RECORDER IS STARTED !! This is done in a free-and-easy way and by a easy comment. It is important to create a light atmosphere and play down the seriousness to make sure that the participants are not oppressed by the situation.

The first question is raised and the group interview is on its way.

The first question is always a "brainstorm" question, and a can affect a lot of immediate attitudes. It is important to give space, be open and listen in the beginning.

On the way

It is not important that all participants answer all questions, but the interviewer should have an impression of what they all think.

If anyone is hiding, the interviewer can always ask "Do you agree, John, or what do you think?"

There will be overlap in questions and answers. Skip questions if they have already been debated and answered

Tick of on the way, when you think that a question have been debated

It is important that all questions are debated. But questions that are more important to the participants than the ones in the interview guide can appear in the discussion and there should always be time to discuss these questions (as long as they are related to the security and privacy debate).

If someone becomes too dominating, it is the interviewers job to bring on the other participants. Ask e.g. "What do the rest of you think?" Interrupt if necessary, it is important that everybody is heard.

If the participants don't say much at the group interview, the interviewer can "take a round" saying that "at the next question I would like to take a round where everybody gives an answer".

Ask for reasons and arguments, "How come you think that… / What is the reason for…

Be aware of the participants reactions; Do they feel comfortable, do they seem under pressure or uneasy etc.

If you are through all the questions before time, you can go back to some of the questions that have not been debated that much on the way.

Closing

When there is 7-8 minutes left, it is a good idea to take a round where everybody gets to make a final remark. The final remark can be things that they have not have the time to state already or points or messages they would like to underline.

You can also ask if something has made a special impression during the conversation.

Annex 5 Frequency tables

5.1 Recoding

To be able to compare education between countries, we have chosen to create a second education variable in accordance with the ISCED-97 standard as presented in "Classifying Educational Programmes – Manual for ISCED-97 Implementation in OECD Countries – 1999 Edition - OECD".

For the cross-tabulations, we have chosen to create binary variables out of age and education, car, e-mail etc. instead of using three or more subgroups. The simple reason is the small datasets – if the statistics gets to detailed, it is impossible to make any useful interpretations of the results.

Accordingly the grouping has been done with three things in mind: 1) To construct groups which have an analytical value, e.g. young/old – high education/low education. 2) To construct groups with enough respondents to make comparison possible. 3) To create groups that are internationally comparable. This means we have tried to identify thresholds for the groups that can be shared by all countries involved.

The groups used in the cross tabulations:

Crosstabs

- Sex: Male / Female
- Age: 50 and above / 49 and below
- Education: Tertiary / non-tertiary
- Children: Yes / no
- Children at home: Yes / no

- Airplane: 1-2 times a year or more / less
- Public: Daily (Also weekly / less for Denmark and Germany)*
- Car: Daily / less (Also weekly / less for Germany)*
- Mobile: Daily / less
- E-mail: Daily / less
- Internet: Daily / less

* We have made additional groupings of these variables, as too few people fit into the ‘daily’ category in these countries.

5.2 Frequencies

Frequencies
Frequency Table

country

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	AT	17	10,8	10,8	10,8
	DE	21	13,3	13,3	24,1
	DK	27	17,1	17,1	41,1
	ES	33	20,9	20,9	62,0
	HU	34	21,5	21,5	83,5
	NO	26	16,5	16,5	100,0
	Total	158	100,0	100,0	

q1sex

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	male	76	48,1	48,1	48,1
	female	82	51,9	51,9	100,0
	Total	158	100,0	100,0	

q3household Persons in houshold ink self

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	38	24,1	24,1	24,1
	2	53	33,5	33,5	57,6
	3	24	15,2	15,2	72,8
	4 or more	43	27,2	27,2	100,0
	Total	158	100,0	100,0	

q4children

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	94	59,5	59,5	59,5
	no	64	40,5	40,5	100,0
	Total	158	100,0	100,0	

q5childhome1 No children

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	61	38,6	38,6	38,6
	yes	97	61,4	61,4	100,0
	Total	158	100,0	100,0	

q5childhome2 14 or younger

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	129	81,6	81,6	81,6
	yes	29	18,4	18,4	100,0
	Total	158	100,0	100,0	

q5childhome3 15 or older

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	124	78,5	78,5	78,5
	yes	34	21,5	21,5	100,0
	Total	158	100,0	100,0	

q6edu

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	,6	,6	,6
	2	17	10,8	10,8	11,4
	3	19	12,0	12,0	23,4
	4	36	22,8	22,8	46,2
	5	21	13,3	13,3	59,5
	6	41	25,9	25,9	85,4
	7	23	14,6	14,6	100,0
	Total	158	100,0	100,0	

q8district

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Metro	127	80,4	80,4	80,4
	Provincial town	18	11,4	11,4	91,8
	Rural	13	8,2	8,2	100,0
	Total	158	100,0	100,0	

q9phone

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	127	80,4	80,4	80,4
	at least once a week	18	11,4	11,4	91,8
	at least once a month	3	1,9	1,9	93,7
	less than once a month	6	3,8	3,8	97,5
	never	4	2,5	2,5	100,0
	Total	158	100,0	100,0	

q10email

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	90	57,0	57,0	57,0
	at least once a week	38	24,1	24,1	81,0
	at least once a month	7	4,4	4,4	85,4
	less than once a month	5	3,2	3,2	88,6
	never	18	11,4	11,4	100,0
	Total	158	100,0	100,0	

q11internet

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	108	68,4	68,4	68,4
	at least once a week	23	14,6	14,6	82,9
	at least once a month	8	5,1	5,1	88,0
	less than once a month	3	1,9	1,9	89,9
	never	16	10,1	10,1	100,0
	Total	158	100,0	100,0	

q12publictransport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	63	39,9	39,9	39,9
	at least once a week	26	16,5	16,5	56,3
	at least once a month	25	15,8	15,8	72,2
	less than once a month	38	24,1	24,1	96,2
	never	6	3,8	3,8	100,0
	Total	158	100,0	100,0	

q13plane

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	more than 5 times a year	15	9,5	9,5	9,5
	3-5 times a year	19	12,0	12,0	21,5
	1-2 times a year	46	29,1	29,1	50,6
	less than 1 time a year	55	34,8	34,8	85,4
	never	23	14,6	14,6	100,0
	Total	158	100,0	100,0	

q14car

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	57	36,1	36,1	36,1
	at least once a week	53	33,5	33,5	69,6
	at least once a month	17	10,8	10,8	80,4
	less than once a month	23	14,6	14,6	94,9
	never	8	5,1	5,1	100,0
	Total	158	100,0	100,0	

q15general The security of society is absolutely dependent on the development and use of new security technologies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	22	13,9	13,9	13,9
	partly agree	59	37,3	37,3	51,3
	neither agree nor disagree	23	14,6	14,6	65,8
	partly disagree	37	23,4	23,4	89,2
	completely disagree	17	10,8	10,8	100,0
	Total	158	100,0	100,0	

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	30	19,0	19,0	19,0
	partly agree	79	50,0	50,0	69,0
	neither agree nor disagree	23	14,6	14,6	83,5
	partly disagree	19	12,0	12,0	95,6
	completely disagree	7	4,4	4,4	100,0
	Total	158	100,0	100,0	

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	22	13,9	13,9	13,9
	partly agree	41	25,9	25,9	39,9
	neither agree nor disagree	10	6,3	6,3	46,2
	partly disagree	42	26,6	26,6	72,8
	completely disagree	43	27,2	27,2	100,0
	Total	158	100,0	100,0	

q18general When security technology is available, we might just as well make use of it

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	33	20,9	20,9	20,9
	partly agree	51	32,3	32,3	53,2
	neither agree nor disagree	20	12,7	12,7	65,8
	partly disagree	29	18,4	18,4	84,2
	completely disagree	25	15,8	15,8	100,0
	Total	158	100,0	100,0	

q19general Privacy should not be violated without reasonable suspicion of criminal intent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	92	58,2	58,2	58,2
	partly agree	42	26,6	26,6	84,8
	neither agree nor disagree	8	5,1	5,1	89,9
	partly disagree	11	7,0	7,0	96,8
	completely disagree	5	3,2	3,2	100,0
	Total	158	100,0	100,0	

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	78	49,4	49,4	49,4
	partly agree	47	29,7	29,7	79,1
	neither agree nor disagree	10	6,3	6,3	85,4
	partly disagree	14	8,9	8,9	94,3
	completely disagree	9	5,7	5,7	100,0
	Total	158	100,0	100,0	

q21general New security technologies are likely to be abused by governmental agencies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	40	25,3	25,3	25,3
	partly agree	58	36,7	36,7	62,0
	neither agree nor disagree	28	17,7	17,7	79,7
	partly disagree	15	9,5	9,5	89,2
	completely disagree	17	10,8	10,8	100,0
	Total	158	100,0	100,0	

q22general New security technologies are likely to be abused by criminals

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	88	55,7	55,7	55,7
	partly agree	50	31,6	31,6	87,3
	neither agree nor disagree	10	6,3	6,3	93,7
	partly disagree	6	3,8	3,8	97,5
	completely disagree	4	2,5	2,5	100,0
	Total	158	100,0	100,0	

q23biom1 Facial characteristics

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	122	77,2	77,7	77,7
	yes	35	22,2	22,3	100,0
	Total	157	99,4	100,0	
Missing	System	1	,6		
Total		158	100,0		

q23biom2 Fingerprints

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	81	51,3	51,3	51,3
	yes	77	48,7	48,7	100,0
	Total	158	100,0	100,0	

q23biom3 Iris recognition

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	111	70,3	70,3	70,3
	yes	47	29,7	29,7	100,0
	Total	158	100,0	100,0	

q23biom4 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	107	67,7	68,2	68,2
	yes	50	31,6	31,8	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q23biom5 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	147	93,0	93,0	93,0
	yes	11	7,0	7,0	100,0
	Total	158	100,0	100,0	

q24biom1 Bank

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	102	64,6	64,6	64,6
	yes	56	35,4	35,4	100,0
	Total	158	100,0	100,0	

q24biom2 Airport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	50	31,6	31,6	31,6
	yes	108	68,4	68,4	100,0
	Total	158	100,0	100,0	

q24biom3 Store

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	147	93,0	93,0	93,0
	yes	11	7,0	7,0	100,0
	Total	158	100,0	100,0	

q24biom4 Border

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	65	41,1	41,1	41,1
	yes	93	58,9	58,9	100,0
	Total	158	100,0	100,0	

q24biom5 Central bus and train station

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	120	75,9	75,9	75,9
	yes	38	24,1	24,1	100,0
	Total	158	100,0	100,0	

q24biom6 Stadium and crowded

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	114	72,2	72,2	72,2
	yes	44	27,8	27,8	100,0
	Total	158	100,0	100,0	

q24biom7 Other private service

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	146	92,4	92,4	92,4
	yes	12	7,6	7,6	100,0
	Total	158	100,0	100,0	

q24biom8 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	125	79,1	79,1	79,1
	yes	33	20,9	20,9	100,0
	Total	158	100,0	100,0	

q24biom9 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	156	98,7	98,7	98,7
	yes	2	1,3	1,3	100,0
	Total	158	100,0	100,0	

q25biom Storing biometric data (e.g. fingerprints or DNA samples) of all citizens in a central database is an acceptable step to fight crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	27	17,1	17,2	17,2
	partly agree	45	28,5	28,7	45,9
	neither agree nor disagree	24	15,2	15,3	61,1
	partly disagree	24	15,2	15,3	76,4
	completely disagree	37	23,4	23,6	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q26biom The use of the biometric passport makes me feel insecure because of the risk of my biometric data being stolen

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	47	29,7	30,1	30,1
	partly agree	49	31,0	31,4	61,5
	neither agree nor disagree	26	16,5	16,7	78,2
	partly disagree	19	12,0	12,2	90,4
	completely disagree	15	9,5	9,6	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q27visual1 Store

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	88	55,7	56,4	56,4
	yes	68	43,0	43,6	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q27visual2 Dressing room

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	145	91,8	92,9	92,9
	yes	11	7,0	7,1	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q27visual3 Central bus and train station

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	58	36,7	37,2	37,2
	yes	98	62,0	62,8	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q27visual4 Bank

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	35	22,2	22,4	22,4
	yes	121	76,6	77,6	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q27visual5 Airport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	13,9	14,1	14,1
	yes	134	84,8	85,9	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q27visual6 Stadium and crowded

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	62	39,2	39,7	39,7
	yes	94	59,5	60,3	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q27visual7 All public

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	117	74,1	75,0	75,0
	yes	39	24,7	25,0	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q27visual8 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	150	94,9	96,2	96,2
	yes	6	3,8	3,8	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q27visual9 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	151	95,6	96,8	96,8
	yes	5	3,2	3,2	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q28visual How do you feel about the number of CCTV cameras in public spaces in general?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	there should be more	50	31,6	36,5	36,5
	the number is appropriate	52	32,9	38,0	74,5
	there should be less	18	11,4	13,1	87,6
	there should be no	17	10,8	12,4	100,0
	Total	137	86,7	100,0	
Missing	d.k.	19	12,0		
	99	2	1,3		
	Total	21	13,3		
Total		158	100,0		

q29visual1 School

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	130	82,3	82,8	82,8
	yes	27	17,1	17,2	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q29visual2 Central bus and train station

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	108	68,4	68,8	68,8
	yes	49	31,0	31,2	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q29visual3 Airport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	10,8	10,8	10,8
	yes	140	88,6	89,2	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q29visual4 Shopping mall

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	139	88,0	88,5	88,5
	yes	18	11,4	11,5	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q29visual5 Public buildings

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	58	36,7	50,9	50,9
	yes	56	35,4	49,1	100,0
	Total	114	72,2	100,0	
Missing	99	44	27,8		
Total		158	100,0		

q29visual6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	148	93,7	94,3	94,3
	yes	9	5,7	5,7	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q29visual7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	151	95,6	96,8	96,8
	yes	5	3,2	3,2	100,0
	Total	156	98,7	100,0	
Missing	99	1	,6		
	System	1	,6		
	Total	2	1,3		
Total		158	100,0		

q30visual1 Reveal everything

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	141	89,2	89,2	89,2
	yes	17	10,8	10,8	100,0
	Total	158	100,0	100,0	

q30visual2 Mannequin projection

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	68	43,0	43,0	43,0
	yes	90	57,0	57,0	100,0
	Total	158	100,0	100,0	

q30visual3 Body heat, sweat & heart rate

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	132	83,5	83,5	83,5
	yes	26	16,5	16,5	100,0
	Total	158	100,0	100,0	

q30visual4 Metal

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	52	32,9	33,1	33,1
	yes	105	66,5	66,9	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q30visual5 Luggage x-ray

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	42	26,6	26,8	26,8
	yes	115	72,8	73,2	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q30visual6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	150	94,9	95,5	95,5
	yes	7	4,4	4,5	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q30visual7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	157	99,4	99,4	99,4
	yes	1	,6	,6	100,0
	Total	158	100,0	100,0	

q31visual CCTV surveillance makes me feel more secure

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	24	15,2	15,2	15,2
	partly agree	71	44,9	44,9	60,1
	neither agree nor disagree	30	19,0	19,0	79,1
	partly disagree	13	8,2	8,2	87,3
	completely disagree	20	12,7	12,7	100,0
	Total	158	100,0	100,0	

q32visual CCTV surveillance infringes my privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	30	19,0	19,0	19,0
	partly agree	63	39,9	39,9	58,9
	neither agree nor disagree	26	16,5	16,5	75,3
	partly disagree	24	15,2	15,2	90,5
	completely disagree	15	9,5	9,5	100,0
	Total	158	100,0	100,0	

q33visual Scanning of persons for detection of hidden items is an acceptable tool for preventing terror

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	50	31,6	31,6	31,6
	partly agree	63	39,9	39,9	71,5
	neither agree nor disagree	10	6,3	6,3	77,8
	partly disagree	18	11,4	11,4	89,2
	completely disagree	17	10,8	10,8	100,0
	Total	158	100,0	100,0	

q34local1 Terrorists and criminals w court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	29	18,4	18,4	18,4
	yes	129	81,6	81,6	100,0
	Total	158	100,0	100,0	

q34local2 Any w/o court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	142	89,9	89,9	89,9
	yes	16	10,1	10,1	100,0
	Total	158	100,0	100,0	

q34local3 Emergency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	13,3	13,3	13,3
	yes	137	86,7	86,7	100,0
	Total	158	100,0	100,0	

q34local4 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	151	95,6	96,2	96,2
	yes	6	3,8	3,8	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q34local5 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	158	100,0	100,0	100,0

q35local1 Terrorists and criminals w court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	31	19,6	20,0	20,0
	yes	124	78,5	80,0	100,0
	Total	155	98,1	100,0	
Missing	99	1	,6		
	System	2	1,3		
	Total	3	1,9		
Total		158	100,0		

q35local2 Any w/o court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	140	88,6	89,2	89,2
	yes	17	10,8	10,8	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q35local3 Stolen vehicles

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	45	28,5	28,7	28,7
	yes	112	70,9	71,3	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q35local4 Speeding

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	124	78,5	79,0	79,0
	yes	33	20,9	21,0	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q35local5 Automatic accident reporting

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	34	21,5	21,7	21,7
	yes	123	77,8	78,3	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q35local6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	152	96,2	96,8	96,8
	yes	5	3,2	3,2	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q35local7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	156	98,7	99,4	99,4
	yes	1	,6	,6	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q36local Should eCall automatically be installed in all new cars?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	33	20,9	21,7	21,7
	yes but possible to deactivate	42	26,6	27,6	49,3
	no, optional	71	44,9	46,7	96,1
	no, never	6	3,8	3,9	100,0
	Total	152	96,2	100,0	
Missing	d.k.	4	2,5		
	99	2	1,3		
	Total	6	3,8		
Total		158	100,0		

q37local The possibility of locating all mobile phones is privacy infringing

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	73	46,2	46,2	46,2
	partly agree	41	25,9	25,9	72,2
	neither agree nor disagree	13	8,2	8,2	80,4
	partly disagree	14	8,9	8,9	89,2
	completely disagree	16	10,1	10,1	99,4
	99	1	,6	,6	100,0
	Total	158	100,0	100,0	

q38local The possibility of locating a suspect's mobile phones is a good tool for the police in investigating and preventing terror and crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	64	40,5	40,5	40,5
	partly agree	56	35,4	35,4	75,9
	neither agree nor disagree	12	7,6	7,6	83,5
	partly disagree	14	8,9	8,9	92,4
	completely disagree	11	7,0	7,0	99,4
	99	1	,6	,6	100,0
	Total	158	100,0	100,0	

q39local The possibility of locating all cars is privacy infringing

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	72	45,6	45,6	45,6
	partly agree	44	27,8	27,8	73,4
	neither agree nor disagree	17	10,8	10,8	84,2
	partly disagree	12	7,6	7,6	91,8
	completely disagree	12	7,6	7,6	99,4
	99	1	,6	,6	100,0
	Total	158	100,0	100,0	

40local The possibility of locating all cars is a good tool for the police in investigatin and preventing terror and crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	37	23,4	23,4	23,4
	partly agree	53	33,5	33,5	57,0
	neither agree nor disagree	25	15,8	15,8	72,8
	partly disagree	18	11,4	11,4	84,2
	completely disagree	24	15,2	15,2	99,4
	99	1	,6	,6	100,0
	Total	158	100,0	100,0	

q41data1 Prevention of terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	79	50,0	50,0	50,0
	yes	79	50,0	50,0	100,0
	Total	158	100,0	100,0	

q41data2 Investigation of terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	61	38,6	38,6	38,6
	yes	97	61,4	61,4	100,0
	Total	158	100,0	100,0	

q41data3 Prevention of crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	95	60,1	60,1	60,1
	yes	63	39,9	39,9	100,0
	Total	158	100,0	100,0	

q41data4 Investigation of crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	65	41,1	41,1	41,1
	yes	93	58,9	58,9	100,0
	Total	158	100,0	100,0	

q41data5 Commercial

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	154	97,5	97,5	97,5
	yes	4	2,5	2,5	100,0
	Total	158	100,0	100,0	

q41data6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	135	85,4	85,4	85,4
	yes	23	14,6	14,6	100,0
	Total	158	100,0	100,0	

q41data7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	151	95,6	95,6	95,6
	yes	7	4,4	4,4	100,0
	Total	158	100,0	100,0	

q42data1 Prevention of terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	86	54,4	54,4	54,4
	yes	72	45,6	45,6	100,0
	Total	158	100,0	100,0	

q42data2 Investigation of terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	59	37,3	37,3	37,3
	yes	99	62,7	62,7	100,0
	Total	158	100,0	100,0	

q42data3 Prevention of crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	100	63,3	63,3	63,3
	yes	58	36,7	36,7	100,0
	Total	158	100,0	100,0	

q42data4 Investigation of crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	53	33,5	33,5	33,5
	yes	105	66,5	66,5	100,0
	Total	158	100,0	100,0	

q42data5 Commercial

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	156	98,7	98,7	98,7
	yes	2	1,3	1,3	100,0
	Total	158	100,0	100,0	

q42data6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	139	88,0	88,0	88,0
	yes	19	12,0	12,0	100,0
	Total	158	100,0	100,0	

q42data7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	152	96,2	96,2	96,2
	yes	6	3,8	3,8	100,0
	Total	158	100,0	100,0	

43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	22	13,9	13,9	13,9
	partly agree	39	24,7	24,7	38,6
	neither agree nor disagree	19	12,0	12,0	50,6
	partly disagree	39	24,7	24,7	75,3
	completely disagree	39	24,7	24,7	100,0
	Total	158	100,0	100,0	

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	72	45,6	45,6	45,6
	partly agree	36	22,8	22,8	68,4
	neither agree nor disagree	21	13,3	13,3	81,6
	partly disagree	25	15,8	15,8	97,5
	completely disagree	4	2,5	2,5	100,0
	Total	158	100,0	100,0	

q45data Scanning of and combining data from different databases containing personal information is privacy infringing

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	82	51,9	51,9	51,9
	partly agree	35	22,2	22,2	74,1
	neither agree nor disagree	18	11,4	11,4	85,4
	partly disagree	17	10,8	10,8	96,2
	completely disagree	6	3,8	3,8	100,0
	Total	158	100,0	100,0	

q46data Scanning of and combining data from different databases is a good tool for police to prevent terror

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	39	24,7	24,7	24,7
	partly agree	45	28,5	28,5	53,2
	neither agree nor disagree	28	17,7	17,7	70,9
	partly disagree	23	14,6	14,6	85,4
	completely disagree	23	14,6	14,6	100,0
	Total	158	100,0	100,0	

ı47data Databases being used for something else than the original purpose is a serious privacy problem

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	127	80,4	80,9	80,9
	partly agree	14	8,9	8,9	89,8
	neither agree nor disagree	5	3,2	3,2	93,0
	partly disagree	4	2,5	2,5	95,5
	completely disagree	7	4,4	4,5	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q48wire1 Prevention and investigation of terrorism w court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	31	19,6	19,6	19,6
	yes	127	80,4	80,4	100,0
	Total	158	100,0	100,0	

q48wire2 Prevention and investigation of terrorism w/o court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	123	77,8	77,8	77,8
	yes	35	22,2	22,2	100,0
	Total	158	100,0	100,0	

q48wire3 Prevention and investigation of crime w court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	24	15,2	15,2	15,2
	yes	134	84,8	84,8	100,0
	Total	158	100,0	100,0	

q48wire4 Prevention and investigation of crime w/o court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	128	81,0	81,0	81,0
	yes	30	19,0	19,0	100,0
	Total	158	100,0	100,0	

q48wire5 Commercial

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	158	100,0	100,0	100,0

q48wire6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	149	94,3	94,3	94,3
	yes	9	5,7	5,7	100,0
	Total	158	100,0	100,0	

q48wire7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	158	100,0	100,0	100,0

q49wire What methods of eavesdropping is acceptable?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	all communication lines	10	6,3	6,7	6,7
	persons that suspect is expected to contact	41	25,9	27,3	34,0
	suspects	84	53,2	56,0	90,0
	totally unacceptable	15	9,5	10,0	100,0
	Total	150	94,9	100,0	
Missing	d.k.	4	2,5		
	99	4	2,5		
	Total	8	5,1		
Total		158	100,0		

q50wire Eavesdropping is a good tool for police investigation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	54	34,2	34,4	34,4
	partly agree	51	32,3	32,5	66,9
	neither agree nor disagree	22	13,9	14,0	80,9
	partly disagree	21	13,3	13,4	94,3
	completely disagree	9	5,7	5,7	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q51wire Eavesdropping is a serious violation of privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	74	46,8	47,1	47,1
	partly agree	45	28,5	28,7	75,8
	neither agree nor disagree	16	10,1	10,2	86,0
	partly disagree	18	11,4	11,5	97,5
	completely disagree	4	2,5	2,5	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q52protect1 Anonymous calling cards

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	91	57,6	58,3	58,3
	yes	65	41,1	41,7	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q52protect2 Encryption programmes

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	69	43,7	44,2	44,2
	yes	87	55,1	55,8	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q52protect3 Identity management

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	86	54,4	55,1	55,1
	yes	70	44,3	44,9	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q52protect4 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	140	88,6	89,7	89,7
	yes	16	10,1	10,3	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q52protect5 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	125	79,1	80,1	80,1
	yes	31	19,6	19,9	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	71	44,9	45,5	45,5
	partly agree	49	31,0	31,4	76,9
	neither agree nor disagree	22	13,9	14,1	91,0
	partly disagree	11	7,0	7,1	98,1
	completely disagree	3	1,9	1,9	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

q54protect Privacy enhancing technologies should not be legal if they make police investigation and prevention of terror and crime more difficult

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	23	14,6	14,6	14,6
	partly agree	36	22,8	22,9	37,6
	neither agree nor disagree	29	18,4	18,5	56,1
	partly disagree	38	24,1	24,2	80,3
	completely disagree	31	19,6	19,7	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q55dilem1 Accept registration of travel and fingerprints

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	138	87,3	87,3	87,3
	yes	20	12,7	12,7	100,0
	Total	158	100,0	100,0	

q55dilem2 Accept only if template

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	143	90,5	90,5	90,5
	yes	15	9,5	9,5	100,0
	Total	158	100,0	100,0	

q55dilem3 Accept only if deleted

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	119	75,3	75,3	75,3
	yes	39	24,7	24,7	100,0
	Total	158	100,0	100,0	

q55dilem4 Accept only if not exclusive

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	92	58,2	58,2	58,2
	yes	66	41,8	41,8	100,0
	Total	158	100,0	100,0	

q55dilem5 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	82	51,9	51,9	51,9
	yes	76	48,1	48,1	100,0
	Total	158	100,0	100,0	

q55dilem6 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	155	98,1	98,1	98,1
	yes	3	1,9	1,9	100,0
	Total	158	100,0	100,0	

q56dilem1 Accept database and biometrics

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	100	63,3	63,3	63,3
	yes	58	36,7	36,7	100,0
	Total	158	100,0	100,0	

q56dilem2 Accept naked machine

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	112	70,9	70,9	70,9
	yes	46	29,1	29,1	100,0
	Total	158	100,0	100,0	

q56dilem3 Accept sweat, body heat and heart rate scanning

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	133	84,2	84,2	84,2
	yes	25	15,8	15,8	100,0
	Total	158	100,0	100,0	

q56dilem4 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	96	60,8	60,8	60,8
	yes	62	39,2	39,2	100,0
	Total	158	100,0	100,0	

q56dilem5 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	144	91,1	91,1	91,1
	yes	14	8,9	8,9	100,0
	Total	158	100,0	100,0	

q57dilem1 Accept all consequences

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	149	94,3	94,3	94,3
	yes	9	5,7	5,7	100,0
	Total	158	100,0	100,0	

q57dilem2 Accept only low rate of false positives

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	131	82,9	82,9	82,9
	yes	27	17,1	17,1	100,0
	Total	158	100,0	100,0	

q57dilem3 Accept only no false positives

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	91	57,6	57,6	57,6
	yes	67	42,4	42,4	100,0
	Total	158	100,0	100,0	

q57dilem4 Accept only in exposed places

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	82	51,9	51,9	51,9
	yes	76	48,1	48,1	100,0
	Total	158	100,0	100,0	

q57dilem5 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	132	83,5	83,5	83,5
	yes	26	16,5	16,5	100,0
	Total	158	100,0	100,0	

q57dilem6 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	152	96,2	96,2	96,2
	yes	6	3,8	3,8	100,0
	Total	158	100,0	100,0	

q58dilem1 Accept all access for counter terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	124	78,5	78,5	78,5
	yes	34	21,5	21,5	100,0
	Total	158	100,0	100,0	

q58dilem2 Accept only if anonymous and w court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	58	36,7	36,7	36,7
	yes	100	63,3	63,3	100,0
	Total	158	100,0	100,0	

q58dilem3 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	128	81,0	81,0	81,0
	yes	30	19,0	19,0	100,0
	Total	158	100,0	100,0	

q58dilem4 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	154	97,5	97,5	97,5
	yes	4	2,5	2,5	100,0
	Total	158	100,0	100,0	

q59dilem1 Accept locate car to prevent crime or terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	80	50,6	51,0	51,0
	yes	77	48,7	49,0	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q59dilem2 Accept speeding tickets

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	149	94,3	94,3	94,3
	yes	9	5,7	5,7	100,0
	Total	158	100,0	100,0	

q59dilem3 Accept register all movements

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	145	91,8	91,8	91,8
	yes	13	8,2	8,2	100,0
	Total	158	100,0	100,0	

q59dilem4 Accept only accidents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	94	59,5	59,5	59,5
	yes	64	40,5	40,5	100,0
	Total	158	100,0	100,0	

q59dilem5 Accept only if voluntary

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	62	39,2	39,2	39,2
	yes	96	60,8	60,8	100,0
	Total	158	100,0	100,0	

q59dilem6 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	158	100,0	100,0	100,0

q60dilem1 Accept calling cards

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	85	53,8	53,8	53,8
	yes	73	46,2	46,2	100,0
	Total	158	100,0	100,0	

q60dilem2 Accept encryption

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	76	48,1	48,1	48,1
	yes	82	51,9	51,9	100,0
	Total	158	100,0	100,0	

q60dilem3 Accept Internet anonymity - bomb

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	106	67,1	67,1	67,1
	yes	52	32,9	32,9	100,0
	Total	158	100,0	100,0	

q60dilem4 Accept Internet anonymity - child pornography

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	131	82,9	82,9	82,9
	yes	27	17,1	17,1	100,0
	Total	158	100,0	100,0	

q60dilem5 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	119	75,3	75,3	75,3
	yes	39	24,7	24,7	100,0
	Total	158	100,0	100,0	

q60dilem6 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	138	87,3	87,3	87,3
	yes	20	12,7	12,7	100,0
	Total	158	100,0	100,0	

q61dilem1 Accept exclusion of refusers from public service

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	135	85,4	86,0	86,0
	yes	22	13,9	14,0	100,0
	Total	157	99,4	100,0	
Missing	System	1	,6		
Total		158	100,0		

q61dilem2 Accept exclusion of unabled from public service

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	146	92,4	92,4	92,4
	yes	12	7,6	7,6	100,0
	Total	158	100,0	100,0	

q61dilem3 Accept refusers are impended when public transport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	117	74,1	74,1	74,1
	yes	41	25,9	25,9	100,0
	Total	158	100,0	100,0	

q61dilem4 Accept unabled are impended when public transport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	143	90,5	90,5	90,5
	yes	15	9,5	9,5	100,0
	Total	158	100,0	100,0	

q61dilem5 Accept no consequences for refusers

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	86	54,4	54,4	54,4
	yes	72	45,6	45,6	100,0
	Total	158	100,0	100,0	

q61dilem6 Accept no consequences for unabled

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	81	51,3	51,3	51,3
	yes	77	48,7	48,7	100,0
	Total	158	100,0	100,0	

q61dilem7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	143	90,5	90,5	90,5
	yes	15	9,5	9,5	100,0
	Total	158	100,0	100,0	

¡62demo Politicians must always submit important questions to public debate and public hearings before making decisions on implementing new security technologies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	103	65,2	65,2	65,2
	partly agree	39	24,7	24,7	89,9
	neither agree nor disagree	7	4,4	4,4	94,3
	partly disagree	9	5,7	5,7	100,0
	Total	158	100,0	100,0	

q63demo The subject of security and privacy is so complicated that it makes no sense to include the general public in discussions of this issue

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	7	4,4	4,4	4,4
	partly agree	20	12,7	12,7	17,1
	neither agree nor disagree	20	12,7	12,7	29,7
	partly disagree	35	22,2	22,2	51,9
	completely disagree	76	48,1	48,1	100,0
	Total	158	100,0	100,0	

q64demo Human rights organisations are always entitled to be heard when important decisions on security and privacy are made

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	103	65,2	65,2	65,2
	partly agree	40	25,3	25,3	90,5
	neither agree nor disagree	11	7,0	7,0	97,5
	partly disagree	3	1,9	1,9	99,4
	completely disagree	1	,6	,6	100,0
	Total	158	100,0	100,0	

q65demo It is important that private companies involved in producing security technologies are also entitled to be heard when important decisions on security and privacy are made

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	50	31,6	31,6	31,6
	partly agree	41	25,9	25,9	57,6
	neither agree nor disagree	33	20,9	20,9	78,5
	partly disagree	15	9,5	9,5	88,0
	completely disagree	19	12,0	12,0	100,0
	Total	158	100,0	100,0	

q66demo In relation to significant decisions on the use of security technologies, it is imperative that alternative solutions are elucidated and included in the debate

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	128	81,0	81,0	81,0
	partly agree	22	13,9	13,9	94,9
	neither agree nor disagree	8	5,1	5,1	100,0
	Total	158	100,0	100,0	

q67suggest Collection of personal data from unsuspicious individuals must be anonymous until identification is authorized by court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	127	80,4	82,5	82,5
	some importance	19	12,0	12,3	94,8
	little importance	5	3,2	3,2	98,1
	not important at all	3	1,9	1,9	100,0
	Total	154	97,5	100,0	
Missing	d.k.	3	1,9		
	99	1	,6		
	Total	4	2,5		
Total		158	100,0		

q68suggest Only authorized personnel can have access to collected personal data

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	148	93,7	94,3	94,3
	some importance	9	5,7	5,7	100,0
	Total	157	99,4	100,0	
Missing	99	1	,6		
Total		158	100,0		

q69suggest Prior to implementing, new security technologies must be checked for privacy impact

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	127	80,4	81,9	81,9
	some importance	26	16,5	16,8	98,7
	little importance	2	1,3	1,3	100,0
	Total	155	98,1	100,0	
Missing	d.k.	3	1,9		
Total		158	100,0		

q70suggest Funding of research projects on new security technologies should be dependent on a thorough analysis of privacy impacts

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	100	63,3	67,1	67,1
	some importance	31	19,6	20,8	87,9
	little importance	13	8,2	8,7	96,6
	not important at all	5	3,2	3,4	100,0
	Total	149	94,3	100,0	
Missing	d.k.	8	5,1		
	99	1	,6		
	Total	9	5,7		
Total		158	100,0		

q71end Have you changed your attitude towards security technologies in general in the course of completing this questionnaire?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes, more positive	20	12,7	13,1	13,1
	yes, more worried	33	20,9	21,6	34,6
	no	100	63,3	65,4	100,0
	Total	153	96,8	100,0	
Missing	d.k.	5	3,2		
Total		158	100,0		

eduISCED97

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	lower secondary level of education	17	10,8	10,8	10,8
	upper secondary level of education	55	34,8	34,8	45,6
	post-secondary non-tertiary	6	3,8	3,8	49,4
	first stage of tertiary education	80	50,6	50,6	100,0
	Total	158	100,0	100,0	

eduISCED97binary Tertiary

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Shorter than tertiary	78	49,4	49,4	49,4
	Tertiary	80	50,6	50,6	100,0
	Total	158	100,0	100,0	

AgeBinary Age over and under 50

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-49	89	56,3	57,1	57,1
	50+	67	42,4	42,9	100,0
	Total	156	98,7	100,0	
Missing	99	2	1,3		
Total		158	100,0		

PhoneBinary Daily

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less	31	19,6	19,6	19,6
	Daily	127	80,4	80,4	100,0
	Total	158	100,0	100,0	

EmailBinary Daily

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less	68	43,0	43,0	43,0
	Daily	90	57,0	57,0	100,0
	Total	158	100,0	100,0	

InternetBinary Daily

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less	50	31,6	31,6	31,6
	Daily	108	68,4	68,4	100,0
	Total	158	100,0	100,0	

PublicBinary Daily

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less	95	60,1	60,1	60,1
	Daily	63	39,9	39,9	100,0
	Total	158	100,0	100,0	

CarBinary Daily

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less	101	63,9	63,9	63,9
	Daily	57	36,1	36,1	100,0
	Total	158	100,0	100,0	

PlaneBinary Less than once a year

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-2 times a year or more	80	50,6	50,6	50,6
	Less than 1 time a year	78	49,4	49,4	100,0
	Total	158	100,0	100,0	

PublicBinary2 Weekly

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	less than once a week	69	43,7	43,7	43,7
	at least once a week	89	56,3	56,3	100,0
	Total	158	100,0	100,0	

CarBinary2 Weekly

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	less than once a week	48	30,4	30,4	30,4
	at least once a week	110	69,6	69,6	100,0
	Total	158	100,0	100,0	

5.3 Cross tables

Crosstabs

15general The security of society is absolutely dependent on the development and use of new securit technologies * q1sex Crosstabulation

			q1sex		
			male	female	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	9	13	22
		% within q1sex	11,8%	15,9%	13,9%
	partly agree	Count	29	30	59
		% within q1sex	38,2%	36,6%	37,3%
	neither agree nor disagree	Count	10	13	23
		% within q1sex	13,2%	15,9%	14,6%
	partly disagree	Count	19	18	37
		% within q1sex	25,0%	22,0%	23,4%
	completely disagree	Count	9	8	17
		% within q1sex	11,8%	9,8%	10,8%
Total		Count	76	82	158
		% within q1sex	100,0%	100,0%	100,0%

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * q1sex Crosstabulation

			q1sex		
			male	female	Total
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	13	17	30
		% within q1sex	17,1%	20,7%	19,0%
	partly agree	Count	44	35	79
		% within q1sex	57,9%	42,7%	50,0%
	neither agree nor disagree	Count	8	15	23
		% within q1sex	10,5%	18,3%	14,6%
	partly disagree	Count	9	10	19
		% within q1sex	11,8%	12,2%	12,0%
	completely disagree	Count	2	5	7
		% within q1sex	2,6%	6,1%	4,4%
Total		Count	76	82	158
		% within q1sex	100,0%	100,0%	100,0%

l7general If you have nothing to hide you don't have to worry about security technologies that infring your privacy * q1sex Crosstabulation

			q1sex		
			male	female	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	11	11	22
		% within q1sex	14,5%	13,4%	13,9%
	partly agree	Count	16	25	41
		% within q1sex	21,1%	30,5%	25,9%
	neither agree nor disagree	Count	4	6	10
		% within q1sex	5,3%	7,3%	6,3%
	partly disagree	Count	23	19	42
		% within q1sex	30,3%	23,2%	26,6%
	completely disagree	Count	22	21	43
		% within q1sex	28,9%	25,6%	27,2%
Total		Count	76	82	158
		% within q1sex	100,0%	100,0%	100,0%

q18general When security technology is available, we might just as well make use of it * q1sex Crosstabulation

			q1sex		
			male	female	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	15	18	33
		% within q1sex	19,7%	22,0%	20,9%
	partly agree	Count	22	29	51
		% within q1sex	28,9%	35,4%	32,3%
	neither agree nor disagree	Count	7	13	20
		% within q1sex	9,2%	15,9%	12,7%
	partly disagree	Count	18	11	29
		% within q1sex	23,7%	13,4%	18,4%
	completely disagree	Count	14	11	25
		% within q1sex	18,4%	13,4%	15,8%
Total		Count	76	82	158
		% within q1sex	100,0%	100,0%	100,0%

q19general Privacy should not be violated without reasonable suspicion of criminal intent * q1sex Crosstabulation

			q1sex		
			male	female	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	41	51	92
		% within q1sex	53,9%	62,2%	58,2%
	partly agree	Count	24	18	42
		% within q1sex	31,6%	22,0%	26,6%
	neither agree nor disagree	Count	5	3	8
		% within q1sex	6,6%	3,7%	5,1%
	partly disagree	Count	5	6	11
		% within q1sex	6,6%	7,3%	7,0%
	completely disagree	Count	1	4	5
		% within q1sex	1,3%	4,9%	3,2%
Total		Count	76	82	158
		% within q1sex	100,0%	100,0%	100,0%

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent * q1sex Crosstabulation

			q1sex		
			male	female	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	40	38	78
		% within q1sex	52,6%	46,3%	49,4%
	partly agree	Count	22	25	47
		% within q1sex	28,9%	30,5%	29,7%
	neither agree nor disagree	Count	4	6	10
		% within q1sex	5,3%	7,3%	6,3%
	partly disagree	Count	7	7	14
		% within q1sex	9,2%	8,5%	8,9%
	completely disagree	Count	3	6	9
		% within q1sex	3,9%	7,3%	5,7%
Total		Count	76	82	158
		% within q1sex	100,0%	100,0%	100,0%

q21general New security technologies are likely to be abused by governmental agencies * q1sex Crosstabulation

			q1sex		
			male	female	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	20	20	40
		% within q1sex	26,3%	24,4%	25,3%
	partly agree	Count	28	30	58
		% within q1sex	36,8%	36,6%	36,7%
	neither agree nor disagree	Count	12	16	28
		% within q1sex	15,8%	19,5%	17,7%
	partly disagree	Count	8	7	15
		% within q1sex	10,5%	8,5%	9,5%
	completely disagree	Count	8	9	17
		% within q1sex	10,5%	11,0%	10,8%
Total		Count	76	82	158
		% within q1sex	100,0%	100,0%	100,0%

q22general New security technologies are likely to be abused by criminals * q1sex Crosstabulation

			q1sex		
			male	female	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	45	43	88
		% within q1sex	59,2%	52,4%	55,7%
	partly agree	Count	23	27	50
		% within q1sex	30,3%	32,9%	31,6%
	neither agree nor disagree	Count	4	6	10
		% within q1sex	5,3%	7,3%	6,3%
	partly disagree	Count	3	3	6
		% within q1sex	3,9%	3,7%	3,8%
	completely disagree	Count	1	3	4
		% within q1sex	1,3%	3,7%	2,5%
Total		Count	76	82	158
		% within q1sex	100,0%	100,0%	100,0%

Crosstabs

q15general The security of society is absolutely dependent on the development and use of new security technologies * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		
			18-49	50+	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	11	11	22
		% within AgeBinary Age over and under 50	12,4%	16,4%	14,1%
	partly agree	Count	36	22	58
		% within AgeBinary Age over and under 50	40,4%	32,8%	37,2%
	neither agree nor disagree	Count	13	10	23
		% within AgeBinary Age over and under 50	14,6%	14,9%	14,7%
	partly disagree	Count	18	19	37
		% within AgeBinary Age over and under 50	20,2%	28,4%	23,7%
	completely disagree	Count	11	5	16
		% within AgeBinary Age over and under 50	12,4%	7,5%	10,3%
Total		Count	89	67	156
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

q16general Many security technologies do not really increase security, but are only being applied to show tha something is done to fight terror * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		
			18-49	50+	Total
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	16	13	29
		% within AgeBinary Age over and under 50	18,0%	19,4%	18,6%
	partly agree	Count	51	27	78
		% within AgeBinary Age over and under 50	57,3%	40,3%	50,0%
	neither agree nor disagree	Count	9	14	23
		% within AgeBinary Age over and under 50	10,1%	20,9%	14,7%
	partly disagree	Count	10	9	19
		% within AgeBinary Age over and under 50	11,2%	13,4%	12,2%
	completely disagree	Count	3	4	7
		% within AgeBinary Age over and under 50	3,4%	6,0%	4,5%
Total		Count	89	67	156
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		
			18-49	50+	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	10	11	21
		% within AgeBinary Age over and under 50	11,2%	16,4%	13,5%
	partly agree	Count	21	20	41
		% within AgeBinary Age over and under 50	23,6%	29,9%	26,3%
	neither agree nor disagree	Count	6	4	10
		% within AgeBinary Age over and under 50	6,7%	6,0%	6,4%
	partly disagree	Count	25	17	42
		% within AgeBinary Age over and under 50	28,1%	25,4%	26,9%
	completely disagree	Count	27	15	42
		% within AgeBinary Age over and under 50	30,3%	22,4%	26,9%
Total		Count	89	67	156
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

¡18general When security technology is available, we might just as well make use of it * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		
			18-49	50+	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	15	18	33
		% within AgeBinary Age over and under 50	16,9%	26,9%	21,2%
	partly agree	Count	28	22	50
		% within AgeBinary Age over and under 50	31,5%	32,8%	32,1%
	neither agree nor disagree	Count	11	9	20
		% within AgeBinary Age over and under 50	12,4%	13,4%	12,8%
	partly disagree	Count	19	10	29
		% within AgeBinary Age over and under 50	21,3%	14,9%	18,6%
	completely disagree	Count	16	8	24
		% within AgeBinary Age over and under 50	18,0%	11,9%	15,4%
Total		Count	89	67	156
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

¡19general Privacy should not be violated without reasonable suspicion of criminal intent * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		
			18-49	50+	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	53	37	90
		% within AgeBinary Age over and under 50	59,6%	55,2%	57,7%
	partly agree	Count	22	20	42
		% within AgeBinary Age over and under 50	24,7%	29,9%	26,9%
	neither agree nor disagree	Count	7	1	8
		% within AgeBinary Age over and under 50	7,9%	1,5%	5,1%
	partly disagree	Count	6	5	11
		% within AgeBinary Age over and under 50	6,7%	7,5%	7,1%
	completely disagree	Count	1	4	5
		% within AgeBinary Age over and under 50	1,1%	6,0%	3,2%
Total		Count	89	67	156
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

20general It is uncomfortable to be under surveillance, even though you have no criminal intent * AgeBinar Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		
			18-49	50+	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	49	27	76
		% within AgeBinary Age over and under 50	55,1%	40,3%	48,7%
	partly agree	Count	25	22	47
		% within AgeBinary Age over and under 50	28,1%	32,8%	30,1%
	neither agree nor disagree	Count	6	4	10
		% within AgeBinary Age over and under 50	6,7%	6,0%	6,4%
	partly disagree	Count	6	8	14
		% within AgeBinary Age over and under 50	6,7%	11,9%	9,0%
	completely disagree	Count	3	6	9
		% within AgeBinary Age over and under 50	3,4%	9,0%	5,8%
Total		Count	89	67	156
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

q21general New security technologies are likely to be abused by governmental agencies * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		
			18-49	50+	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	25	15	40
		% within AgeBinary Age over and under 50	28,1%	22,4%	25,6%
	partly agree	Count	33	25	58
		% within AgeBinary Age over and under 50	37,1%	37,3%	37,2%
	neither agree nor disagree	Count	16	10	26
		% within AgeBinary Age over and under 50	18,0%	14,9%	16,7%
	partly disagree	Count	8	7	15
		% within AgeBinary Age over and under 50	9,0%	10,4%	9,6%
	completely disagree	Count	7	10	17
		% within AgeBinary Age over and under 50	7,9%	14,9%	10,9%
Total		Count	89	67	156
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

q22general New security technologies are likely to be abused by criminals * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		
			18-49	50+	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	50	37	87
		% within AgeBinary Age over and under 50	56,2%	55,2%	55,8%
	partly agree	Count	29	21	50
		% within AgeBinary Age over and under 50	32,6%	31,3%	32,1%
	neither agree nor disagree	Count	4	5	9
		% within AgeBinary Age over and under 50	4,5%	7,5%	5,8%
	partly disagree	Count	5	1	6
		% within AgeBinary Age over and under 50	5,6%	1,5%	3,8%
	completely disagree	Count	1	3	4
		% within AgeBinary Age over and under 50	1,1%	4,5%	2,6%
Total		Count	89	67	156
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

Crosstabs

q15general The security of society is absolutely dependent on the development and use of new security technologies * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	12	10	22
		% within eduISCED97binary Tertiary	15,4%	12,5%	13,9%
	partly agree	Count	33	26	59
		% within eduISCED97binary Tertiary	42,3%	32,5%	37,3%
	neither agree nor disagree	Count	10	13	23
		% within eduISCED97binary Tertiary	12,8%	16,3%	14,6%
	partly disagree	Count	16	21	37
		% within eduISCED97binary Tertiary	20,5%	26,3%	23,4%
	completely disagree	Count	7	10	17
		% within eduISCED97binary Tertiary	9,0%	12,5%	10,8%
Total		Count	78	80	158
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

16general Many security technologies do not really increase security, but are only being applied to show tha something is done to fight terror * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	19	11	30
		% within eduISCED97binary Tertiary	24,4%	13,8%	19,0%
	partly agree	Count	34	45	79
		% within eduISCED97binary Tertiary	43,6%	56,3%	50,0%
	neither agree nor disagree	Count	14	9	23
		% within eduISCED97binary Tertiary	17,9%	11,3%	14,6%
	partly disagree	Count	9	10	19
		% within eduISCED97binary Tertiary	11,5%	12,5%	12,0%
	completely disagree	Count	2	5	7
		% within eduISCED97binary Tertiary	2,6%	6,3%	4,4%
Total		Count	78	80	158
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

¡17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	15	7	22
		% within eduISCED97binary Tertiary	19,2%	8,8%	13,9%
	partly agree	Count	22	19	41
		% within eduISCED97binary Tertiary	28,2%	23,8%	25,9%
	neither agree nor disagree	Count	4	6	10
		% within eduISCED97binary Tertiary	5,1%	7,5%	6,3%
	partly disagree	Count	22	20	42
		% within eduISCED97binary Tertiary	28,2%	25,0%	26,6%
	completely disagree	Count	15	28	43
		% within eduISCED97binary Tertiary	19,2%	35,0%	27,2%
Total		Count	78	80	158
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

q18general When security technology is available, we might just as well make use of it * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	23	10	33
		% within eduISCED97binary Tertiary	29,5%	12,5%	20,9%
	partly agree	Count	25	26	51
		% within eduISCED97binary Tertiary	32,1%	32,5%	32,3%
	neither agree nor disagree	Count	11	9	20
		% within eduISCED97binary Tertiary	14,1%	11,3%	12,7%
	partly disagree	Count	12	17	29
		% within eduISCED97binary Tertiary	15,4%	21,3%	18,4%
	completely disagree	Count	7	18	25
		% within eduISCED97binary Tertiary	9,0%	22,5%	15,8%
Total		Count	78	80	158
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

q19general Privacy should not be violated without reasonable suspicion of criminal intent * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	55	37	92
		% within eduISCED97binary Tertiary	70,5%	46,3%	58,2%
	partly agree	Count	13	29	42
		% within eduISCED97binary Tertiary	16,7%	36,3%	26,6%
	neither agree nor disagree	Count	2	6	8
		% within eduISCED97binary Tertiary	2,6%	7,5%	5,1%
	partly disagree	Count	7	4	11
		% within eduISCED97binary Tertiary	9,0%	5,0%	7,0%
	completely disagree	Count	1	4	5
		% within eduISCED97binary Tertiary	1,3%	5,0%	3,2%
Total		Count	78	80	158
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	45	33	78
		% within eduISCED97binary Tertiary	57,7%	41,3%	49,4%
	partly agree	Count	14	33	47
		% within eduISCED97binary Tertiary	17,9%	41,3%	29,7%
	neither agree nor disagree	Count	6	4	10
		% within eduISCED97binary Tertiary	7,7%	5,0%	6,3%
	partly disagree	Count	9	5	14
		% within eduISCED97binary Tertiary	11,5%	6,3%	8,9%
	completely disagree	Count	4	5	9
		% within eduISCED97binary Tertiary	5,1%	6,3%	5,7%
Total		Count	78	80	158
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

q21general New security technologies are likely to be abused by governmental agencies * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	18	22	40
		% within eduISCED97binary Tertiary	23,1%	27,5%	25,3%
	partly agree	Count	34	24	58
		% within eduISCED97binary Tertiary	43,6%	30,0%	36,7%
	neither agree nor disagree	Count	10	18	28
		% within eduISCED97binary Tertiary	12,8%	22,5%	17,7%
	partly disagree	Count	8	7	15
		% within eduISCED97binary Tertiary	10,3%	8,8%	9,5%
	completely disagree	Count	8	9	17
		% within eduISCED97binary Tertiary	10,3%	11,3%	10,8%
Total		Count	78	80	158
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

q22general New security technologies are likely to be abused by criminals * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	43	45	88
		% within eduISCED97binary Tertiary	55,1%	56,3%	55,7%
	partly agree	Count	21	29	50
		% within eduISCED97binary Tertiary	26,9%	36,3%	31,6%
	neither agree nor disagree	Count	7	3	10
		% within eduISCED97binary Tertiary	9,0%	3,8%	6,3%
	partly disagree	Count	5	1	6
		% within eduISCED97binary Tertiary	6,4%	1,3%	3,8%
	completely disagree	Count	2	2	4
		% within eduISCED97binary Tertiary	2,6%	2,5%	2,5%
Total		Count	78	80	158
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

Crosstabs

q15general The security of society is absolutely dependent on the development and use of new security technologies * q4children Crosstabulation

			q4children		
			yes	no	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	17	5	22
		% within q4children	18,1%	7,8%	13,9%
	partly agree	Count	37	22	59
		% within q4children	39,4%	34,4%	37,3%
	neither agree nor disagree	Count	10	13	23
		% within q4children	10,6%	20,3%	14,6%
	partly disagree	Count	24	13	37
		% within q4children	25,5%	20,3%	23,4%
	completely disagree	Count	6	11	17
		% within q4children	6,4%	17,2%	10,8%
Total		Count	94	64	158
		% within q4children	100,0%	100,0%	100,0%

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * q4children Crosstabulation

			q4children		
			yes	no	Total
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	18	12	30
		% within q4children	19,1%	18,8%	19,0%
	partly agree	Count	47	32	79
		% within q4children	50,0%	50,0%	50,0%
	neither agree nor disagree	Count	13	10	23
		% within q4children	13,8%	15,6%	14,6%
	partly disagree	Count	11	8	19
		% within q4children	11,7%	12,5%	12,0%
	completely disagree	Count	5	2	7
		% within q4children	5,3%	3,1%	4,4%
Total		Count	94	64	158
		% within q4children	100,0%	100,0%	100,0%

.7general If you have nothing to hide you don't have to worry about security technologies that infringe you privacy * q4children Crosstabulation

			q4children		
			yes	no	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	12	10	22
		% within q4children	12,8%	15,6%	13,9%
	partly agree	Count	31	10	41
		% within q4children	33,0%	15,6%	25,9%
	neither agree nor disagree	Count	8	2	10
		% within q4children	8,5%	3,1%	6,3%
	partly disagree	Count	23	19	42
		% within q4children	24,5%	29,7%	26,6%
	completely disagree	Count	20	23	43
		% within q4children	21,3%	35,9%	27,2%
Total		Count	94	64	158
		% within q4children	100,0%	100,0%	100,0%

q18general When security technology is available, we might just as well make use of it * q4children Crosstabulation

			q4children		
			yes	no	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	23	10	33
		% within q4children	24,5%	15,6%	20,9%
	partly agree	Count	34	17	51
		% within q4children	36,2%	26,6%	32,3%
	neither agree nor disagree	Count	9	11	20
		% within q4children	9,6%	17,2%	12,7%
	partly disagree	Count	17	12	29
		% within q4children	18,1%	18,8%	18,4%
	completely disagree	Count	11	14	25
		% within q4children	11,7%	21,9%	15,8%
Total		Count	94	64	158
		% within q4children	100,0%	100,0%	100,0%

q19general Privacy should not be violated without reasonable suspicion of criminal intent * q4children Crosstabulation

			q4children		
			yes	no	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	56	36	92
		% within q4children	59,6%	56,3%	58,2%
	partly agree	Count	24	18	42
		% within q4children	25,5%	28,1%	26,6%
	neither agree nor disagree	Count	3	5	8
		% within q4children	3,2%	7,8%	5,1%
	partly disagree	Count	7	4	11
		% within q4children	7,4%	6,3%	7,0%
	completely disagree	Count	4	1	5
		% within q4children	4,3%	1,6%	3,2%
Total		Count	94	64	158
		% within q4children	100,0%	100,0%	100,0%

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent * q4children Crosstabulation

			q4children		
			yes	no	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	46	32	78
		% within q4children	48,9%	50,0%	49,4%
	partly agree	Count	27	20	47
		% within q4children	28,7%	31,3%	29,7%
	neither agree nor disagree	Count	5	5	10
		% within q4children	5,3%	7,8%	6,3%
	partly disagree	Count	11	3	14
		% within q4children	11,7%	4,7%	8,9%
	completely disagree	Count	5	4	9
		% within q4children	5,3%	6,3%	5,7%
Total		Count	94	64	158
		% within q4children	100,0%	100,0%	100,0%

q21general New security technologies are likely to be abused by governmental agencies * q4children Crosstabulation

			q4children		
			yes	no	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	22	18	40
		% within q4children	23,4%	28,1%	25,3%
	partly agree	Count	37	21	58
		% within q4children	39,4%	32,8%	36,7%
	neither agree nor disagree	Count	16	12	28
		% within q4children	17,0%	18,8%	17,7%
	partly disagree	Count	8	7	15
		% within q4children	8,5%	10,9%	9,5%
	completely disagree	Count	11	6	17
		% within q4children	11,7%	9,4%	10,8%
Total		Count	94	64	158
		% within q4children	100,0%	100,0%	100,0%

q22general New security technologies are likely to be abused by criminals * q4children Crosstabulation

			q4children		
			yes	no	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	53	35	88
		% within q4children	56,4%	54,7%	55,7%
	partly agree	Count	27	23	50
		% within q4children	28,7%	35,9%	31,6%
	neither agree nor disagree	Count	6	4	10
		% within q4children	6,4%	6,3%	6,3%
	partly disagree	Count	4	2	6
		% within q4children	4,3%	3,1%	3,8%
	completely disagree	Count	4	0	4
		% within q4children	4,3%	,0%	2,5%
Total		Count	94	64	158
		% within q4children	100,0%	100,0%	100,0%

Crosstabs

q15general The security of society is absolutely dependent on the development and use of new security technologies * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	12	10	22
		% within q5childhome1 No children	19,7%	10,3%	13,9%
	partly agree	Count	24	35	59
		% within q5childhome1 No children	39,3%	36,1%	37,3%
	neither agree nor disagree	Count	6	17	23
		% within q5childhome1 No children	9,8%	17,5%	14,6%
	partly disagree	Count	16	21	37
		% within q5childhome1 No children	26,2%	21,6%	23,4%
	completely disagree	Count	3	14	17
		% within q5childhome1 No children	4,9%	14,4%	10,8%
Total		Count	61	97	158
		% within q5childhome1 No children	100,0%	100,0%	100,0%

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	11	19	30
		% within q5childhome1 No children	18,0%	19,6%	19,0%
	partly agree	Count	33	46	79
		% within q5childhome1 No children	54,1%	47,4%	50,0%
	neither agree nor disagree	Count	8	15	23
		% within q5childhome1 No children	13,1%	15,5%	14,6%
	partly disagree	Count	7	12	19
		% within q5childhome1 No children	11,5%	12,4%	12,0%
	completely disagree	Count	2	5	7
		% within q5childhome1 No children	3,3%	5,2%	4,4%
Total		Count	61	97	158
		% within q5childhome1 No children	100,0%	100,0%	100,0%

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	10	12	22
		% within q5childhome1 No children	16,4%	12,4%	13,9%
	partly agree	Count	16	25	41
		% within q5childhome1 No children	26,2%	25,8%	25,9%
	neither agree nor disagree	Count	6	4	10
		% within q5childhome1 No children	9,8%	4,1%	6,3%
	partly disagree	Count	16	26	42
		% within q5childhome1 No children	26,2%	26,8%	26,6%
	completely disagree	Count	13	30	43
		% within q5childhome1 No children	21,3%	30,9%	27,2%
Total		Count	61	97	158
		% within q5childhome1 No children	100,0%	100,0%	100,0%

18general When security technology is available, we might just as well make use of it * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	15	18	33
		% within q5childhome1 No children	24,6%	18,6%	20,9%
	partly agree	Count	19	32	51
		% within q5childhome1 No children	31,1%	33,0%	32,3%
	neither agree nor disagree	Count	9	11	20
		% within q5childhome1 No children	14,8%	11,3%	12,7%
	partly disagree	Count	10	19	29
		% within q5childhome1 No children	16,4%	19,6%	18,4%
	completely disagree	Count	8	17	25
		% within q5childhome1 No children	13,1%	17,5%	15,8%
Total		Count	61	97	158
		% within q5childhome1 No children	100,0%	100,0%	100,0%

19general Privacy should not be violated without reasonable suspicion of criminal intent * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	37	55	92
		% within q5childhome1 No children	60,7%	56,7%	58,2%
	partly agree	Count	14	28	42
		% within q5childhome1 No children	23,0%	28,9%	26,6%
	neither agree nor disagree	Count	3	5	8
		% within q5childhome1 No children	4,9%	5,2%	5,1%
	partly disagree	Count	5	6	11
		% within q5childhome1 No children	8,2%	6,2%	7,0%
	completely disagree	Count	2	3	5
		% within q5childhome1 No children	3,3%	3,1%	3,2%
Total		Count	61	97	158
		% within q5childhome1 No children	100,0%	100,0%	100,0%

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	31	47	78
		% within q5childhome1 No children	50,8%	48,5%	49,4%
	partly agree	Count	16	31	47
		% within q5childhome1 No children	26,2%	32,0%	29,7%
	neither agree nor disagree	Count	4	6	10
		% within q5childhome1 No children	6,6%	6,2%	6,3%
	partly disagree	Count	6	8	14
		% within q5childhome1 No children	9,8%	8,2%	8,9%
	completely disagree	Count	4	5	9
		% within q5childhome1 No children	6,6%	5,2%	5,7%
Total		Count	61	97	158
		% within q5childhome1 No children	100,0%	100,0%	100,0%

q21general New security technologies are likely to be abused by governmental agencies * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	14	26	40
		% within q5childhome1 No children	23,0%	26,8%	25,3%
	partly agree	Count	24	34	58
		% within q5childhome1 No children	39,3%	35,1%	36,7%
	neither agree nor disagree	Count	13	15	28
		% within q5childhome1 No children	21,3%	15,5%	17,7%
	partly disagree	Count	2	13	15
		% within q5childhome1 No children	3,3%	13,4%	9,5%
	completely disagree	Count	8	9	17
		% within q5childhome1 No children	13,1%	9,3%	10,8%
Total		Count	61	97	158
		% within q5childhome1 No children	100,0%	100,0%	100,0%

q22general New security technologies are likely to be abused by criminals * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	36	52	88
		% within q5childhome1 No children	59,0%	53,6%	55,7%
	partly agree	Count	15	35	50
		% within q5childhome1 No children	24,6%	36,1%	31,6%
	neither agree nor disagree	Count	5	5	10
		% within q5childhome1 No children	8,2%	5,2%	6,3%
	partly disagree	Count	3	3	6
		% within q5childhome1 No children	4,9%	3,1%	3,8%
	completely disagree	Count	2	2	4
		% within q5childhome1 No children	3,3%	2,1%	2,5%
Total		Count	61	97	158
		% within q5childhome1 No children	100,0%	100,0%	100,0%

Crosstabs

q24biom2 Airport * PlaneBinary Less than once a year Crosstabulation

			PlaneBinary Less than once a year		
			1-2 times a year or more	Less than 1 time a year	Total
q24biom2 Airport	no	Count	29	21	50
		% within PlaneBinary Less than once a year	36,3%	26,9%	31,6%
	yes	Count	51	57	108
		% within PlaneBinary Less than once a year	63,8%	73,1%	68,4%
Total		Count	80	78	158
		% within PlaneBinary Less than once a year	100,0%	100,0%	100,0%

Crosstabs

q56dilem1 Accept database and biometrics * PlaneBinary Less than once a year Crosstabulation

			PlaneBinary Less than once a year		
			1-2 times a year or more	Less than 1 time a year	Total
q56dilem1 Accept database and biometrics	no	Count	44	56	100
		% within PlaneBinary Less than once a year	55,0%	71,8%	63,3%
	yes	Count	36	22	58
		% within PlaneBinary Less than once a year	45,0%	28,2%	36,7%
Total		Count	80	78	158
		% within PlaneBinary Less than once a year	100,0%	100,0%	100,0%

Crosstabs

q24biom5 Central bus and train station * PublicBinary Daily Crosstabulation

			PublicBinary Daily		
			Less	Daily	Total
q24biom5 Central bus and train station	no	Count	74	46	120
		% within PublicBinary Daily	77,9%	73,0%	75,9%
	yes	Count	21	17	38
		% within PublicBinary Daily	22,1%	27,0%	24,1%
Total		Count	95	63	158
		% within PublicBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q55dilem1 Accept registration of travel and fingerprints * PublicBinary Daily Crosstabulation

			PublicBinary Daily		
			Less	Daily	Total
q55dilem1 Accept registration of travel and fingerprints	no	Count	82	56	138
		% within PublicBinary Daily	86,3%	88,9%	87,3%
	yes	Count	13	7	20
		% within PublicBinary Daily	13,7%	11,1%	12,7%
Total		Count	95	63	158
		% within PublicBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q35local1 Terrorists and criminals w court order * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q35local1 Terrorists and criminals w court order	no	Count	20	11	31
		% within CarBinary Daily	20,4%	19,3%	20,0%
	yes	Count	78	46	124
		% within CarBinary Daily	79,6%	80,7%	80,0%
Total		Count	98	57	155
		% within CarBinary Daily	100,0%	100,0%	100,0%

q35local2 Any w/o court order * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q35local2 Any w/o court order	no	Count	91	49	140
		% within CarBinary Daily	91,0%	86,0%	89,2%
	yes	Count	9	8	17
		% within CarBinary Daily	9,0%	14,0%	10,8%
Total		Count	100	57	157
		% within CarBinary Daily	100,0%	100,0%	100,0%

q35local3 Stolen vehicles * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q35local3 Stolen vehicles	no	Count	29	16	45
		% within CarBinary Daily	29,0%	28,1%	28,7%
	yes	Count	71	41	112
		% within CarBinary Daily	71,0%	71,9%	71,3%
Total		Count	100	57	157
		% within CarBinary Daily	100,0%	100,0%	100,0%

q35local4 Speeding * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q35local4 Speeding	no	Count	79	45	124
		% within CarBinary Daily	79,0%	78,9%	79,0%
	yes	Count	21	12	33
		% within CarBinary Daily	21,0%	21,1%	21,0%
Total		Count	100	57	157
		% within CarBinary Daily	100,0%	100,0%	100,0%

q35local5 Automatic accident reporting * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q35local5 Automatic accident reporting	no	Count	22	12	34
		% within CarBinary Daily	22,0%	21,1%	21,7%
	yes	Count	78	45	123
		% within CarBinary Daily	78,0%	78,9%	78,3%
Total		Count	100	57	157
		% within CarBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q36local Should eCall automatically be installed in all new cars? * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q36local Should eCall automatically be installed in all new cars?	yes	Count	18	15	33
		% within CarBinary Daily	18,9%	26,3%	21,7%
	yes but possible to deactivate	Count	28	14	42
		% within CarBinary Daily	29,5%	24,6%	27,6%
	no, optional	Count	46	25	71
		% within CarBinary Daily	48,4%	43,9%	46,7%
	no, never	Count	3	3	6
		% within CarBinary Daily	3,2%	5,3%	3,9%
Total		Count	95	57	152
		% within CarBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q39local The possibility of locating all cars is privacy infringing * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q39local The possibility of locating all cars is privacy infringing	completely agree	Count	46	26	72
		% within CarBinary Daily	45,5%	45,6%	45,6%
	partly agree	Count	28	16	44
		% within CarBinary Daily	27,7%	28,1%	27,8%
	neither agree nor disagree	Count	12	5	17
		% within CarBinary Daily	11,9%	8,8%	10,8%
	partly disagree	Count	6	6	12
		% within CarBinary Daily	5,9%	10,5%	7,6%
	completely disagree	Count	8	4	12
		% within CarBinary Daily	7,9%	7,0%	7,6%
	99	Count	1	0	1
		% within CarBinary Daily	1,0%	,0%	,6%
Total		Count	101	57	158
		% within CarBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q59dilem1 Accept locate car to prevent crime or terrorism * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q59dilem1 Accept locate car to prevent crime or terrorism	no	Count	53	27	80
		% within CarBinary Daily	52,5%	48,2%	51,0%
	yes	Count	48	29	77
		% within CarBinary Daily	47,5%	51,8%	49,0%
Total		Count	101	56	157
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem2 Accept speeding tickets * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q59dilem2 Accept speeding tickets	no	Count	92	57	149
		% within CarBinary Daily	91,1%	100,0%	94,3%
	yes	Count	9	0	9
		% within CarBinary Daily	8,9%	,0%	5,7%
Total		Count	101	57	158
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem3 Accept register all movements * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q59dilem3 Accept register all movements	no	Count	94	51	145
		% within CarBinary Daily	93,1%	89,5%	91,8%
	yes	Count	7	6	13
		% within CarBinary Daily	6,9%	10,5%	8,2%
Total		Count	101	57	158
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem4 Accept only accidents * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q59dilem4 Accept only accidents	no	Count	57	37	94
		% within CarBinary Daily	56,4%	64,9%	59,5%
	yes	Count	44	20	64
		% within CarBinary Daily	43,6%	35,1%	40,5%
Total		Count	101	57	158
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem5 Accept only if voluntary * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q59dilem5 Accept only if voluntary	no	Count	40	22	62
		% within CarBinary Daily	39,6%	38,6%	39,2%
	yes	Count	61	35	96
		% within CarBinary Daily	60,4%	61,4%	60,8%
Total		Count	101	57	158
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem6 d.k. * CarBinary Daily Crosstabulation

		CarBinary Daily		
		Less	Daily	Total
q59dilem6 d.k. no	Count	101	57	158
	% within CarBinary Daily	100,0%	100,0%	100,0%
Total	Count	101	57	158
	% within CarBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary	completely agree	Count	2	20	22
		% within PhoneBinary Daily	6,5%	15,7%	13,9%
	partly agree	Count	7	32	39
		% within PhoneBinary Daily	22,6%	25,2%	24,7%
	neither agree nor disagree	Count	3	16	19
		% within PhoneBinary Daily	9,7%	12,6%	12,0%
	partly disagree	Count	8	31	39
		% within PhoneBinary Daily	25,8%	24,4%	24,7%
	completely disagree	Count	11	28	39
		% within PhoneBinary Daily	35,5%	22,0%	24,7%
Total		Count	31	127	158
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

ı43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary * EmailBinary Daily Crosstabulation

			EmailBinary Daily		
			Less	Daily	Total
q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary	completely agree	Count	14	8	22
		% within EmailBinary Daily	20,6%	8,9%	13,9%
	partly agree	Count	13	26	39
		% within EmailBinary Daily	19,1%	28,9%	24,7%
	neither agree nor disagree	Count	10	9	19
		% within EmailBinary Daily	14,7%	10,0%	12,0%
	partly disagree	Count	16	23	39
		% within EmailBinary Daily	23,5%	25,6%	24,7%
	completely disagree	Count	15	24	39
		% within EmailBinary Daily	22,1%	26,7%	24,7%
Total		Count	68	90	158
		% within EmailBinary Daily	100,0%	100,0%	100,0%

43data Government institutions should store all data they find necessary for security reasons for as long a they consider it necessary * InternetBinary Daily Crosstabulation

			InternetBinary Daily		
			Less	Daily	Total
q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary	completely agree	Count	12	10	22
		% within InternetBinary Daily	24,0%	9,3%	13,9%
	partly agree	Count	9	30	39
		% within InternetBinary Daily	18,0%	27,8%	24,7%
	neither agree nor disagree	Count	9	10	19
		% within InternetBinary Daily	18,0%	9,3%	12,0%
	partly disagree	Count	12	27	39
		% within InternetBinary Daily	24,0%	25,0%	24,7%
	completely disagree	Count	8	31	39
		% within InternetBinary Daily	16,0%	28,7%	24,7%
Total		Count	50	108	158
		% within InternetBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count	18	54	72
		% within PhoneBinary Daily	58,1%	42,5%	45,6%
	partly agree	Count	4	32	36
		% within PhoneBinary Daily	12,9%	25,2%	22,8%
	neither agree nor disagree	Count	3	18	21
		% within PhoneBinary Daily	9,7%	14,2%	13,3%
	partly disagree	Count	4	21	25
		% within PhoneBinary Daily	12,9%	16,5%	15,8%
	completely disagree	Count	2	2	4
		% within PhoneBinary Daily	6,5%	1,6%	2,5%
Total		Count	31	127	158
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes * EmailBinary Daily Crosstabulation

			EmailBinary Daily		
			Less	Daily	Total
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count	34	38	72
		% within EmailBinary Daily	50,0%	42,2%	45,6%
	partly agree	Count	15	21	36
		% within EmailBinary Daily	22,1%	23,3%	22,8%
	neither agree nor disagree	Count	11	10	21
		% within EmailBinary Daily	16,2%	11,1%	13,3%
	partly disagree	Count	5	20	25
		% within EmailBinary Daily	7,4%	22,2%	15,8%
	completely disagree	Count	3	1	4
		% within EmailBinary Daily	4,4%	1,1%	2,5%
Total		Count	68	90	158
		% within EmailBinary Daily	100,0%	100,0%	100,0%

44data Data from phone, mobile and Internet communication should not be stored beyond what is neede for billing purposes * InternetBinary Daily Crosstabulation

			InternetBinary Daily		
			Less	Daily	Total
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count	23	49	72
		% within InternetBinary Daily	46,0%	45,4%	45,6%
	partly agree	Count	12	24	36
		% within InternetBinary Daily	24,0%	22,2%	22,8%
	neither agree nor disagree	Count	7	14	21
		% within InternetBinary Daily	14,0%	13,0%	13,3%
	partly disagree	Count	6	19	25
		% within InternetBinary Daily	12,0%	17,6%	15,8%
	completely disagree	Count	2	2	4
		% within InternetBinary Daily	4,0%	1,9%	2,5%
Total		Count	50	108	158
		% within InternetBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q45data Scanning of and combining data from different databases containing personal information is privacy infringing * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count	23	59	82
		% within PhoneBinary Daily	74,2%	46,5%	51,9%
	partly agree	Count	4	31	35
		% within PhoneBinary Daily	12,9%	24,4%	22,2%
	neither agree nor disagree	Count	1	17	18
		% within PhoneBinary Daily	3,2%	13,4%	11,4%
	partly disagree	Count	2	15	17
		% within PhoneBinary Daily	6,5%	11,8%	10,8%
	completely disagree	Count	1	5	6
		% within PhoneBinary Daily	3,2%	3,9%	3,8%
Total		Count	31	127	158
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q45data Scanning of and combining data from different databases containing personal information is privacy infringing * EmailBinary Daily Crosstabulation

			EmailBinary Daily		
			Less	Daily	Total
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count	36	46	82
		% within EmailBinary Daily	52,9%	51,1%	51,9%
	partly agree	Count	16	19	35
		% within EmailBinary Daily	23,5%	21,1%	22,2%
	neither agree nor disagree	Count	10	8	18
		% within EmailBinary Daily	14,7%	8,9%	11,4%
	partly disagree	Count	3	14	17
		% within EmailBinary Daily	4,4%	15,6%	10,8%
	completely disagree	Count	3	3	6
		% within EmailBinary Daily	4,4%	3,3%	3,8%
Total		Count	68	90	158
		% within EmailBinary Daily	100,0%	100,0%	100,0%

q45data Scanning of and combining data from different databases containing personal information is privacy infringing * InternetBinary Daily Crosstabulation

			InternetBinary Daily		
			Less	Daily	Total
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count	24	58	82
		% within InternetBinary Daily	48,0%	53,7%	51,9%
	partly agree	Count	14	21	35
		% within InternetBinary Daily	28,0%	19,4%	22,2%
	neither agree nor disagree	Count	6	12	18
		% within InternetBinary Daily	12,0%	11,1%	11,4%
	partly disagree	Count	3	14	17
		% within InternetBinary Daily	6,0%	13,0%	10,8%
	completely disagree	Count	3	3	6
		% within InternetBinary Daily	6,0%	2,8%	3,8%
Total		Count	50	108	158
		% within InternetBinary Daily	100,0%	100,0%	100,0%

Crosstabs

47data Databases being used for something else than the original purpose is a serious privacy problem * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q47data Databases being used for something else than the original purpose is a serious privacy problem	completely agree	Count	25	102	127
		% within PhoneBinary Daily	80,6%	81,0%	80,9%
	partly agree	Count	2	12	14
		% within PhoneBinary Daily	6,5%	9,5%	8,9%
	neither agree nor disagree	Count	1	4	5
		% within PhoneBinary Daily	3,2%	3,2%	3,2%
	partly disagree	Count	1	3	4
		% within PhoneBinary Daily	3,2%	2,4%	2,5%
	completely disagree	Count	2	5	7
		% within PhoneBinary Daily	6,5%	4,0%	4,5%
Total		Count	31	126	157
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

47data Databases being used for something else than the original purpose is a serious privacy problem * EmailBinary Daily Crosstabulation

			EmailBinary Daily		
			Less	Daily	Total
q47data Databases being used for something else than the original purpose is a serious privacy problem	completely agree	Count	58	69	127
		% within EmailBinary Daily	86,6%	76,7%	80,9%
	partly agree	Count	2	12	14
		% within EmailBinary Daily	3,0%	13,3%	8,9%
	neither agree nor disagree	Count	2	3	5
		% within EmailBinary Daily	3,0%	3,3%	3,2%
	partly disagree	Count	1	3	4
		% within EmailBinary Daily	1,5%	3,3%	2,5%
	completely disagree	Count	4	3	7
		% within EmailBinary Daily	6,0%	3,3%	4,5%
Total		Count	67	90	157
		% within EmailBinary Daily	100,0%	100,0%	100,0%

q47data Databases being used for something else than the original purpose is a serious privacy problem * InternetBinary Daily Crosstabulation

			InternetBinary Daily		
			Less	Daily	Total
q47data Databases being used for something else than the original purpose is a serious privacy problem	completely agree	Count	44	83	127
		% within InternetBinary Daily	88,0%	77,6%	80,9%
	partly agree	Count	1	13	14
		% within InternetBinary Daily	2,0%	12,1%	8,9%
	neither agree nor disagree	Count	1	4	5
		% within InternetBinary Daily	2,0%	3,7%	3,2%
	partly disagree	Count	1	3	4
		% within InternetBinary Daily	2,0%	2,8%	2,5%
	completely disagree	Count	3	4	7
		% within InternetBinary Daily	6,0%	3,7%	4,5%
Total		Count	50	107	157
		% within InternetBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q51wire Eavesdropping is a serious violation of privacy * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count	20	54	74
		% within PhoneBinary Daily	64,5%	42,9%	47,1%
	partly agree	Count	5	40	45
		% within PhoneBinary Daily	16,1%	31,7%	28,7%
	neither agree nor disagree	Count	3	13	16
		% within PhoneBinary Daily	9,7%	10,3%	10,2%
	partly disagree	Count	2	16	18
		% within PhoneBinary Daily	6,5%	12,7%	11,5%
	completely disagree	Count	1	3	4
		% within PhoneBinary Daily	3,2%	2,4%	2,5%
Total		Count	31	126	157
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q51wire Eavesdropping is a serious violation of privacy * EmailBinary Daily Crosstabulation

			EmailBinary Daily		
			Less	Daily	Total
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count	34	40	74
		% within EmailBinary Daily	50,0%	44,9%	47,1%
	partly agree	Count	20	25	45
		% within EmailBinary Daily	29,4%	28,1%	28,7%
	neither agree nor disagree	Count	6	10	16
		% within EmailBinary Daily	8,8%	11,2%	10,2%
	partly disagree	Count	5	13	18
		% within EmailBinary Daily	7,4%	14,6%	11,5%
	completely disagree	Count	3	1	4
		% within EmailBinary Daily	4,4%	1,1%	2,5%
Total		Count	68	89	157
		% within EmailBinary Daily	100,0%	100,0%	100,0%

q51wire Eavesdropping is a serious violation of privacy * InternetBinary Daily Crosstabulation

			InternetBinary Daily		
			Less	Daily	Total
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count	24	50	74
		% within InternetBinary Daily	48,0%	46,7%	47,1%
	partly agree	Count	15	30	45
		% within InternetBinary Daily	30,0%	28,0%	28,7%
	neither agree nor disagree	Count	5	11	16
		% within InternetBinary Daily	10,0%	10,3%	10,2%
	partly disagree	Count	3	15	18
		% within InternetBinary Daily	6,0%	14,0%	11,5%
	completely disagree	Count	3	1	4
		% within InternetBinary Daily	6,0%	,9%	2,5%
Total		Count	50	107	157
		% within InternetBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count	15	56	71
		% within PhoneBinary Daily	50,0%	44,4%	45,5%
	partly agree	Count	7	42	49
		% within PhoneBinary Daily	23,3%	33,3%	31,4%
	neither agree nor disagree	Count	6	16	22
		% within PhoneBinary Daily	20,0%	12,7%	14,1%
	partly disagree	Count	2	9	11
		% within PhoneBinary Daily	6,7%	7,1%	7,1%
	completely disagree	Count	0	3	3
		% within PhoneBinary Daily	,0%	2,4%	1,9%
Total		Count	30	126	156
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy * EmailBinary Daily Crosstabulation

			EmailBinary Daily		
			Less	Daily	Total
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count	34	37	71
		% within EmailBinary Daily	50,7%	41,6%	45,5%
	partly agree	Count	19	30	49
		% within EmailBinary Daily	28,4%	33,7%	31,4%
	neither agree nor disagree	Count	12	10	22
		% within EmailBinary Daily	17,9%	11,2%	14,1%
	partly disagree	Count	2	9	11
		% within EmailBinary Daily	3,0%	10,1%	7,1%
	completely disagree	Count	0	3	3
		% within EmailBinary Daily	,0%	3,4%	1,9%
Total		Count	67	89	156
		% within EmailBinary Daily	100,0%	100,0%	100,0%

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy * InternetBinary Daily Crosstabulation

			InternetBinary Daily		
			Less	Daily	Total
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count	23	48	71
		% within InternetBinary Daily	46,9%	44,9%	45,5%
	partly agree	Count	16	33	49
		% within InternetBinary Daily	32,7%	30,8%	31,4%
	neither agree nor disagree	Count	8	14	22
		% within InternetBinary Daily	16,3%	13,1%	14,1%
	partly disagree	Count	2	9	11
		% within InternetBinary Daily	4,1%	8,4%	7,1%
	completely disagree	Count	0	3	3
		% within InternetBinary Daily	,0%	2,8%	1,9%
Total		Count	49	107	156
		% within InternetBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q58dilem1 Accept all access for counter terrorism * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q58dilem1 Accept all access for counter terrorism	no	Count	26	98	124
		% within PhoneBinary Daily	83,9%	77,2%	78,5%
	yes	Count	5	29	34
		% within PhoneBinary Daily	16,1%	22,8%	21,5%
Total		Count	31	127	158
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q58dilem1 Accept all access for counter terrorism * EmailBinary Daily Crosstabulation

			EmailBinary Daily		
			Less	Daily	Total
q58dilem1 Accept all access for counter terrorism	no	Count	51	73	124
		% within EmailBinary Daily	75,0%	81,1%	78,5%
	yes	Count	17	17	34
		% within EmailBinary Daily	25,0%	18,9%	21,5%
Total		Count	68	90	158
		% within EmailBinary Daily	100,0%	100,0%	100,0%

q58dilem1 Accept all access for counter terrorism * InternetBinary Daily Crosstabulation

			InternetBinary Daily		
			Less	Daily	Total
q58dilem1 Accept all access for counter terrorism	no	Count	34	90	124
		% within InternetBinary Daily	68,0%	83,3%	78,5%
	yes	Count	16	18	34
		% within InternetBinary Daily	32,0%	16,7%	21,5%
Total		Count	50	108	158
		% within InternetBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q34local1 Terrorists and criminals w court order * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q34local1 Terrorists and criminals w court order	no	Count	3	26	29
		% within PhoneBinary Daily	9,7%	20,5%	18,4%
	yes	Count	28	101	129
		% within PhoneBinary Daily	90,3%	79,5%	81,6%
Total		Count	31	127	158
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q34local2 Any w/o court order * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q34local2 Any w/o court order	no	Count	28	114	142
		% within PhoneBinary Daily	90,3%	89,8%	89,9%
	yes	Count	3	13	16
		% within PhoneBinary Daily	9,7%	10,2%	10,1%
Total		Count	31	127	158
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q34local3 Emergency * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q34local3 Emergency	no	Count	5	16	21
		% within PhoneBinary Daily	16,1%	12,6%	13,3%
	yes	Count	26	111	137
		% within PhoneBinary Daily	83,9%	87,4%	86,7%
Total		Count	31	127	158
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q34local4 Never * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q34local4 Never	no	Count	30	121	151
		% within PhoneBinary Daily	96,8%	96,0%	96,2%
	yes	Count	1	5	6
		% within PhoneBinary Daily	3,2%	4,0%	3,8%
Total		Count	31	126	157
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q34local5 d.k. * PhoneBinary Daily Crosstabulation

		PhoneBinary Daily		
		Less	Daily	Total
q34local5 d.k. no	Count	31	127	158
	% within PhoneBinary Daily	100,0%	100,0%	100,0%
Total	Count	31	127	158
	% within PhoneBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q52protect1 Anonymous calling cards * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q52protect1 Anonymous calling cards	no	Count	11	80	91
		% within PhoneBinary Daily	36,7%	63,5%	58,3%
	yes	Count	19	46	65
		% within PhoneBinary Daily	63,3%	36,5%	41,7%
Total		Count	30	126	156
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q37local The possibility of locating all mobile phones is privacy infringing * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q37local The possibility of locating all mobile phones is privacy infringing	completely agree	Count	18	55	73
		% within PhoneBinary Daily	58,1%	43,3%	46,2%
	partly agree	Count	6	35	41
		% within PhoneBinary Daily	19,4%	27,6%	25,9%
	neither agree nor disagree	Count	2	11	13
		% within PhoneBinary Daily	6,5%	8,7%	8,2%
	partly disagree	Count	0	14	14
		% within PhoneBinary Daily	,0%	11,0%	8,9%
	completely disagree	Count	4	12	16
		% within PhoneBinary Daily	12,9%	9,4%	10,1%
	99	Count	1	0	1
		% within PhoneBinary Daily	3,2%	,0%	,6%
Total		Count	31	127	158
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q52protect2 Encryption programmes * EmailBinary Daily Crosstabulation

			EmailBinary Daily		
			Less	Daily	Total
q52protect2 Encryption programmes	no	Count	29	40	69
		% within EmailBinary Daily	43,3%	44,9%	44,2%
	yes	Count	38	49	87
		% within EmailBinary Daily	56,7%	55,1%	55,8%
Total		Count	67	89	156
		% within EmailBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q52protect3 Identity management * InternetBinary Daily Crosstabulation

			InternetBinary Daily		
			Less	Daily	Total
q52protect3 Identity management	no	Count	26	60	86
		% within InternetBinary Daily	53,1%	56,1%	55,1%
	yes	Count	23	47	70
		% within InternetBinary Daily	46,9%	43,9%	44,9%
Total		Count	49	107	156
		% within InternetBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q24biom5 Central bus and train station * PublicBinary2 Weekly Crosstabulation

			PublicBinary2 Weekly		
			less than once a week	at least once a week	Total
q24biom5 Central bus and train station	no	Count	52	68	120
		% within PublicBinary2 Weekly	75,4%	76,4%	75,9%
	yes	Count	17	21	38
		% within PublicBinary2 Weekly	24,6%	23,6%	24,1%
Total		Count	69	89	158
		% within PublicBinary2 Weekly	100,0%	100,0%	100,0%

Crosstabs

q35local1 Terrorists and criminals w court order * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		
			less than once a week	at least once a week	Total
q35local1 Terrorists and criminals w court order	no	Count	8	23	31
		% within CarBinary2 Weekly	17,0%	21,3%	20,0%
	yes	Count	39	85	124
		% within CarBinary2 Weekly	83,0%	78,7%	80,0%
Total		Count	47	108	155
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q35local2 Any w/o court order * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		
			less than once a week	at least once a week	Total
q35local2 Any w/o court order	no	Count	44	96	140
		% within CarBinary2 Weekly	91,7%	88,1%	89,2%
	yes	Count	4	13	17
		% within CarBinary2 Weekly	8,3%	11,9%	10,8%
Total		Count	48	109	157
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q35local3 Stolen vehicles * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		
			less than once a week	at least once a week	Total
q35local3 Stolen vehicles	no	Count	13	32	45
		% within CarBinary2 Weekly	27,1%	29,4%	28,7%
	yes	Count	35	77	112
		% within CarBinary2 Weekly	72,9%	70,6%	71,3%
Total		Count	48	109	157
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q35local4 Speeding * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		
			less than once a week	at least once a week	Total
q35local4 Speeding	no	Count	38	86	124
		% within CarBinary2 Weekly	79,2%	78,9%	79,0%
	yes	Count	10	23	33
		% within CarBinary2 Weekly	20,8%	21,1%	21,0%
Total		Count	48	109	157
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q35local5 Automatic accident reporting * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		
			less than once a week	at least once a week	Total
q35local5 Automatic accident reporting	no	Count	10	24	34
		% within CarBinary2 Weekly	20,8%	22,0%	21,7%
	yes	Count	38	85	123
		% within CarBinary2 Weekly	79,2%	78,0%	78,3%
Total		Count	48	109	157
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

Crosstabs

q36local Should eCall automatically be installed in all new cars? * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		
			less than once a week	at least once a week	Total
q36local Should eCall automatically be installed in all new cars?	yes	Count	8	25	33
		% within CarBinary2 Weekly	17,4%	23,6%	21,7%
	yes but possible to deactivate	Count	15	27	42
		% within CarBinary2 Weekly	32,6%	25,5%	27,6%
	no, optional	Count	22	49	71
		% within CarBinary2 Weekly	47,8%	46,2%	46,7%
	no, never	Count	1	5	6
		% within CarBinary2 Weekly	2,2%	4,7%	3,9%
Total		Count	46	106	152
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

Crosstabs

q39local The possibility of locating all cars is privacy infringing * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		
			less than once a week	at least once a week	Total
q39local The possibility of locating all cars is privacy infringing	completely agree	Count	18	54	72
		% within CarBinary2 Weekly	37,5%	49,1%	45,6%
	partly agree	Count	18	26	44
		% within CarBinary2 Weekly	37,5%	23,6%	27,8%
	neither agree nor disagree	Count	4	13	17
		% within CarBinary2 Weekly	8,3%	11,8%	10,8%
	partly disagree	Count	3	9	12
		% within CarBinary2 Weekly	6,3%	8,2%	7,6%
	completely disagree	Count	5	7	12
		% within CarBinary2 Weekly	10,4%	6,4%	7,6%
	99	Count	0	1	1
		% within CarBinary2 Weekly	,0%	,9%	,6%
Total		Count	48	110	158
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

Crosstabs

q59dilem1 Accept locate car to prevent crime or terrorism * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		
			less than once a week	at least once a week	Total
q59dilem1 Accept locate car to prevent crime or terrorism	no	Count	28	52	80
		% within CarBinary2 Weekly	58,3%	47,7%	51,0%
	yes	Count	20	57	77
		% within CarBinary2 Weekly	41,7%	52,3%	49,0%
Total		Count	48	109	157
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q59dilem2 Accept speeding tickets * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		
			less than once a week	at least once a week	Total
q59dilem2 Accept speeding tickets	no	Count	44	105	149
		% within CarBinary2 Weekly	91,7%	95,5%	94,3%
	yes	Count	4	5	9
		% within CarBinary2 Weekly	8,3%	4,5%	5,7%
Total		Count	48	110	158
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q59dilem3 Accept register all movements * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		
			less than once a week	at least once a week	Total
q59dilem3 Accept register all movements	no	Count	45	100	145
		% within CarBinary2 Weekly	93,8%	90,9%	91,8%
	yes	Count	3	10	13
		% within CarBinary2 Weekly	6,3%	9,1%	8,2%
Total		Count	48	110	158
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q59dilem4 Accept only accidents * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		
			less than once a week	at least once a week	Total
q59dilem4 Accept only accidents	no	Count	23	71	94
		% within CarBinary2 Weekly	47,9%	64,5%	59,5%
	yes	Count	25	39	64
		% within CarBinary2 Weekly	52,1%	35,5%	40,5%
Total		Count	48	110	158
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q59dilem5 Accept only if voluntary * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		
			less than once a week	at least once a week	Total
q59dilem5 Accept only if voluntary	no	Count	18	44	62
		% within CarBinary2 Weekly	37,5%	40,0%	39,2%
	yes	Count	30	66	96
		% within CarBinary2 Weekly	62,5%	60,0%	60,8%
Total		Count	48	110	158
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q59dilem6 d.k. * CarBinary2 Weekly Crosstabulation

		CarBinary2 Weekly		
		less than once a week	at least once a week	Total
q59dilem6 d.k. no	Count	48	110	158
	% within CarBinary2 Weekly	100,0%	100,0%	100,0%
Total	Count	48	110	158
	% within CarBinary2 Weekly	100,0%	100,0%	100,0%

5.4 Syntax / SPSS

```
***recoding***

RECODE
  eduISCED97
  (5 thru 6=1)  (ELSE=0)  INTO  eduISCED97binary .
VARIABLE LABELS eduISCED97binary 'Tertiary'.
EXECUTE .

RECODE
  q2age
  (17 thru 49=0)  (50 thru 90=1)  (MISSING=Copy)  INTO  AgeBinary .
VARIABLE LABELS AgeBinary 'Age over and under 50'.
EXECUTE .

RECODE
  q9phone q10email q11internet q12publictransport q14car
  (1=1)  (2 thru 5=0)  INTO  PhoneBinary  EmailBinary  InternetBinary  PublicBinary  CarBinary
.
VARIABLE  LABELS  PhoneBinary  'Daily'  /EmailBinary  'Daily'  /InternetBinary  'Daily'
/PublicBinary 'Daily' /CarBinary 'Daily'.
EXECUTE .

RECODE
  q12publictransport q14car
  (1 thru 2=1)  (3 thru 5=0)  INTO  PublicBinary2  CarBinary2 .
VARIABLE LABELS PublicBinary2 'Weekly' /CarBinary2 'Weekly'.
EXECUTE .

RECODE
  q13plane
  (4 thru 5=1)  (1 thru 3=0)  INTO  PlaneBinary .
VARIABLE LABELS PlaneBinary 'Less than once a year'.
EXECUTE .

RECODE
  q2age
  (Lowest thru 34=1)  (35 thru 54=2)  (55 thru 98=3)  INTO  Agein3Groups .
VARIABLE LABELS Agein3Groups 'Age in 3 Groups'.
EXECUTE .

***crosstabs general attitude***

CROSSTABS
  /TABLES=q15general q16general q17general q18general q19general q20general q21general
q22general BY q1sex
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q15general q16general q17general q18general q19general q20general q21general
q22general BY AgeBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLUMN
  /COUNT ROUND CELL .
```

```
CROSSTABS
  /TABLES=q15general q16general q17general q18general q19general q20general q21general
q22general BY eduISCED97binary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q15general q16general q17general q18general q19general q20general q21general
q22general BY q4children
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q15general q16general q17general q18general q19general q20general q21general
q22general BY q5childhome1
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLUMN
  /COUNT ROUND CELL .

***crosstabs 2***

CROSSTABS
  /TABLES=q24biom2  BY PlaneBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q56dilem1 BY PlaneBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q24biom5  BY PublicBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q55dilem1 BY PublicBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q35local1 q35local2 q35local3 q35local4 q35local5 BY CarBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q36local BY CarBinary
  /FORMAT= AVALUE TABLES
```

```
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q39local BY CarBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q59dilem1 q59dilem2 q59dilem3 q59dilem4 q59dilem5 q59dilem6 BY CarBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q43data BY PhoneBinary EmailBinary InternetBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q44data BY PhoneBinary EmailBinary InternetBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q45data BY PhoneBinary EmailBinary InternetBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q47data BY PhoneBinary EmailBinary InternetBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q51wire BY PhoneBinary EmailBinary InternetBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q53protect BY PhoneBinary EmailBinary InternetBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q58dilem1 BY PhoneBinary EmailBinary InternetBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL
```

```
CROSSTABS
  /TABLES=q34local1 q34local2 q34local3 q34local4 q34local5 BY PhoneBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q52protect1 BY PhoneBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q37local BY PhoneBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q52protect2 BY EmailBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .

CROSSTABS
  /TABLES=q52protect3 BY InternetBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLOUMN
  /COUNT ROUND CELL .
```