Project acronym:	PRISMS
Project title:	The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making
Project number:	285399
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2011.6.5-2: The relationship between Human privacy and security
Contract type:	Collaborative project
Start date of project:	01 February 2012
Duration:	42 months

Deliverable 7.1: Report on Existing Surveys

Editors:	Hayley Watson, David Wright (Trilateral Research & Consulting)
Contributors:	David Wright, Hayley Watson, Rachel L. Finn (Trilateral Research & Consulting), Iván Székely (EKINT), Charles D. Raab (University of Edinburgh), Kerstin Goos, Michael Friedewald (Fraunhofer ISI)
Reviewer:	Gideon Skinner (Ipsos MORI)

Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Due date:	31 January 2013
Submission date:	14 March 2013

About the PRISMS project

The PRISMS project analyses the traditional trade-off model between privacy and security and devise a more evidence-based perspective for reconciling privacy and security, trust and concern. It examines how technologies aimed at enhancing security are subjecting citizens to an increasing amount of surveillance and, in many cases, causing infringements of privacy and fundamental rights. It conducts both a multidisciplinary inquiry into the concepts of privacy and security and their relationships and an EU-wide survey to determine whether people evaluate the introduction of security technologies in terms of a trade-off. As a result, the project determines the factors that affect public assessment of the security and privacy implications of a given security technology. The project uses these results to devise a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account a wider society context.

Terms of use

Document history

Version	Date	Changes
1.0	14 March 2013	First version of deliverable

Table of Contents

EXECUTIVE SUMMARY

Understanding citizens' construction of the trade-off between privacy and security requires an examination of how privacy, security, trust and surveillance are understood by members of the public in Europe and elsewhere. Academics have found that the concepts of privacy and security are notoriously difficult to define. Although policy documents, academic literature and mainstream media materials offer some definitions of each of these concepts, there is often little connection between the way that professionals in each of these fields and members of the public understand these concepts.

The PRISMS project involves analysing the traditional trade-off model between privacy and security and devising a more evidence-based perspective for reconciling privacy and security, trust and concern. The aim of the present report is to present findings from the five tasks completed in PRISMS work package seven surrounding the analysis of existing surveys, the results of which will be used to inform the development of the PRISMS survey.

What follows is an executive summary of the various chapters within this report:

Chapter 2: Analysis of existing public opinion surveys: Methodology
Chapter two provides further information regarding the data collection process for the analysis of existing surveys in chapter four. The chapter provides a meta-analysis of the collection of surveys providing details as to the number of surveys, the subject area, who conducted the survey, who the surveys were conducted for, information regarding the sample size and the methodologies employed to conduct the surveys. The analysis revealed that as a short term research aim, when planning and conducting the PRISMS survey it is necessary to be transparent in the methodological design and reasons for conducting the survey within the dissemination and final write-up of the report. In the longer term, the PRISMS surveys needs to further explore the effects of interests and agents, as well as their interdependence in creating and using public opinion surveys in our research area. The chapter then goes on to provide information regarding the methodology and details regarding the smaller sample of surveys (taken from this initial sample) and used for the comparative analysis of existing surveys in chapter four.

Chapter 3: Meta-analysis
The aim of chapter three was to take stock of existing surveys (identified in chapter two and assessed in greater detail in chapter four) at the intersection of surveillance and privacy, to consider them from a methodological standpoint of good practice, to evaluate their reliability and comparability, and to draw lessons from this exercise. This permits an assessment of the quality of surveys, enabling PRISMS to make recommendations regarding methodological considerations for conducting its own survey.

Partners identified several methodological issues relating to the reliability and comparability of existing surveys: Methodological problems: non-response, issues concerning demographic variables, the diverse meanings of privacy, data gathering techniques and response rate; comparative problems: frequent failure to describe fully, and in some reasonably standard way, the methods used in conducting the survey, including sampling procedure and issues associated with methodological transparency, where there was evidence of a lack of reporting of response rates, inclusion of the questionnaire in the final report.

The chapter concludes with a series of recommendations to be considered in the construction of the PRISMS survey: the size and range of the PRISMS survey should be directly comparable to the Eurobarometer surveys of privacy-related topics conducted in all the countries of the EU; the inclusion of contextual and personal questions (identified in chapter 6) relating to the daily lives of respondents that could influence their responses.

Chapter 4: Analysis of existing public opinion surveys
Chapter four aims to provide an examination of what 20 public opinion surveys on privacy, trust, security and surveillance have revealed about citizens' perceptions of these issues. In addition, this analysis of surveys aims to provide an indication of what (if any) measures citizens are choosing to take to enhance their security, privacy and trust. Section 4.1 through to 4.20 of this report presents the results of the comparative analysis of existing surveys where partners identified: the methodology used, the main findings of the survey, the surveys relationship with other surveys and any information regarding the external use of the survey's results (e.g., within the news media or within policy).

Chapter 5: Horizontal analysis
Drawing on the results of chapter four, chapter five proceeds to provide a horizontal analysis of public attitudes towards the four themes being assessed (privacy, trust, security and surveillance). The findings reveal that citizens are willing to give up some aspects of their privacy in the face of some surveillance technologies deployed to enhance their security. However, this does not necessarily mean that citizens trust the institutions implementing these measures.

More specifically, with regard to privacy, findings from the surveys point towards citizens having been consistently concerned about privacy from 1997 to the present. The comparative analysis of existing surveys shows that some individuals are taking measures to try to enhance their privacy. Examples of favourable measures include: refusing to provide personal information to companies and government, asking a company not to sell information, asking a company to remove their data from its marketing list and reading online privacy policies. Examples of less favourable measures to enhance privacy include: purposefully giving false information and asking to see what information was held on record. Reasons as to "why" these options were less favourable were not provided. Future research needs to explore all seven types of privacy, and that researchers should try to ask why respondents are or are not concerned with different types of privacy. Future research may also want to determine the different measures people use to protect their online privacy including asking respondents how successful they feel they are in maintaining and managing their privacy.

In relation to trust, in general, individuals claim that they are not entirely trusting of others' ability to correctly handle their personal data. Individuals were more likely to trust public organisations and institutes more than private companies. Future surveys should try to understand whether trust of organisations has any impact on public attitudes towards forgoing privacy to enhance security. Future surveys ought to try and develop questions that seek to further understand why individuals do not trust certain organisations, and what they feel can be done to improve their trust. Surveys should also try to understand how trusting individuals are of different surveillance technologies and those who operate them.

With regard to security, findings from some surveys have revealed that some individuals are willing to "trade" their privacy, by supporting some surveillance measures to protect their physical security, however, this is certainly not straightforward, and results are dependent on

the type of surveillance technology, as well as who is being placed under surveillance. Alternatively, when considering public attitudes towards cyber security, some surveys revealed that individuals are concerned about threats they may face relating to their personal data. The surveys have provided some indication of what measures individuals choose to take in order to protect themselves online. Respondents were particularly attracted to measures that were readily accessible, rather than more practical steps that they would have to explicitly and actively choose. Future research ought to try to develop a more comprehensive understanding of the various measures people are choosing to take, or avoiding to take and, crucially, why they are making these decisions.

In relation to public attitudes of surveillance technologies in society, eight surveys provide evidence that some individuals respond positively to the use of surveillance measures to help enhance their security. Whilst some individuals claim that they support the presence of surveillance technologies in their lives to help enhance their security, others believe that the use of surveillance measures by organisations and companies should be limited due to privacy concerns. Surveys do not always try to understand the relationship between surveillance and privacy. However, those surveys that do consider this issue have found that people are often uncomfortable with technologies that intrude upon the privacy of their bodies (e.g., biometrics, DNA, body scanners) and privacy of their communications (e.g., e-mail and telephone monitoring). Many respondents were also concerned about where visual surveillance technologies such as CCTV cameras are placed and where their images are displayed. In relation to European Member States, with the exception of Greece, all European states show greater objection to being surveyed in private spaces than in public spaces. Future research must continue to try to understand the relationship between public perceptions of different types of surveillance technologies and what this implies for people's sense of privacy.

The horizontal analysis also assessed demographic, temporal and technology differences in results. The surveys demonstrate that variables such as location, gender, age and education have had a noticeable impact on public attitudes. Alternatively, location did play a role in relation to public attitudes concerning trusting others with their data. For example, those in Central and Eastern Europe were found to be less trusting than those in the UK and Ireland, Denmark, France and the Netherlands. In relation to temporal differences, the surveys reveal that citizens' concern over privacy has changed somewhat over time; Results from the 2008 Flash Eurobarometer show that in comparison to 2003, those in Denmark, Germany, Spain, Austria and Portugal have experienced a vast growth in the number of citizens who are concerned with the privacy of their data held by organisations, whilst those in Greece, the Netherlands, Finland and Sweden have seen a decline in concern. However, citizens appear to be developing greater trust in the ability of public organisations to manage their personal information. One key temporal difference is that people do not have enough knowledge about the impact of new technologies on their privacy, resulting in this lack of knowledge amplifying their concern about privacy. Finally, as mentioned above, this analysis has revealed that the type of surveillance technology under discussion has an impact on public attitudes towards surveillance, and the technology involved as well as the target of the surveillance measure heavily influence people's level of support for them.

Chapter 6: Short comings & lessons learned

Chapter six aims to consider any shortcomings or limitations of those surveys that may provide lessons for the design of the PRISMS survey. Partners note extraneous and situational

factors that may influence responses, including media portrayals, cultural differences, knowledge of privacy laws and specific events.

Findings suggested that it is important for future surveys to consider the question of "why" respondents feel the way they do about privacy, trust, security and surveillance. Additionally, as also identified in chapter five, it is useful to be able to make comparisons at the demographic level. Partners' findings also suggested that it is useful to compare and contrast findings from previous surveys, and to use previous question techniques as well as new areas of consideration to further develop future surveys relating to privacy, trust, security and surveillance. Consequently, partners have identified a series of six suggestions to include new types of questions in the planned PRISMS survey. These additional questions should explore: personal life history, religious or philosophical beliefs, belonging to minority groups, offline communication / social contacts, bad (and good) personal experience and other sensitive personal data.

The chapter concluded with a series of hypotheses to be considered in the development of the PRISMS survey.

1. Characteristics of the respondents' personal life history have a significant correlation with the respondents' opinion on, and attitudes towards, privacy, security, trust and surveillance.
2. The existence and characteristics of religious or philosophical beliefs (including the characteristics of the religion or church in question) show correlations with the respondents' opinion on, and attitudes towards, privacy, security, trust and surveillance.
3. Belonging to ethnic, religious, cultural, sexual or other minorities in society also have a measurable impact on people's view on the borderlines of private and public life. Similarly, other sensitive personal data (health status, pathological addictions, sexual preferences, criminal convictions etc.) may also show correlations with the distribution of survey data. These correlations are bi-directional: belonging to a minority group, or having an illness do not necessarily result in a higher sensitivity to privacy.
4. Not only online communication habits but also offline communication experience, including participation in social events, exchange of news and information, the nature of information shared with others, and the expectations of what should and what should not be divulged about the respondent's private life in the various social circles, show correlations with the respondents' views on privacy and related subject areas.

Chapter 7: Analysis of social values surveys

Chapter seven aims to consider the potential disparities of the prospective respondents with regard to their attitudes towards privacy, security and trust in relation to their cultural roots. The chapter reviews the concept of 'cultural values' and its roots within the social sciences. The chapter involves an exploratory analysis of existing cultural values surveys: the European Values Survey, the World Values Survey and the European Social Survey. The chapter then proceeds to presenting the results of an exploratory analysis of European differences in terms of culturally related perceptions of privacy and security and related concepts.

Results of the analysis revealed that privacy, security and trust are approached in both a direct and indirect manner in social values surveys. Privacy is approached indirectly; trust directly and security directly and indirectly. Personal autonomy and individualism are concepts that have been covered by the surveys and are helpful to draw on in relation to privacy. Our analysis of social values surveys revealed that the surveys approach to operationalising

privacy and security is somewhat different to those surveys analysed in previous tasks, where in social values surveys focus is placed on direct and indirect types of privacy and security.

The chapter concludes with a series of hypothesis, relating to the inclusion of questions surrounding social values, to be considered in the development of the PRISMS survey:

1. The higher the socio economic status of a citizen, the more important privacy is.
2. The economic development of a country determines citizen's perceived need for security mechanisms.
3. Security is always important, but the focus is different dependent on the higher the income.
4. The religion of a citizen influences an individual's perception of privacy.
5. In those parts of Europe where interpersonal trust is low, citizens are willing to give up privacy for a potential increase in security.

Chapter 8: Recommended questions

Chapter eight aims to review and analyse survey question techniques and provide a set of hypothesis and related questions to support the construction of the PRISMS survey. With regard to the operationalisation of concepts the surveys assessed in this task examined five out of seven types of privacy classified by Finn et al.: privacy of the person, privacy of behaviour and action, privacy of communication, privacy of data and image and privacy of location and space. Of these five, the surveys assessed in this analysis predominantly focus their attention on privacy of data and image. In the surveys analysed, trust is commonly defined in relation to the privacy of data and images, where individuals are asked whether they trust others to secure their personal data. The surveys assessed in this task only address three out of seven types of security classified by Lagazio: physical, radical uncertainty and cyber and information security. The surveys assessed in this report did not provide an indication of how individuals felt about physical security; instead, questions were commonly limited to whether respondents approved of increasing surveillance measures. The majority of surveys (nine out of 12) directly refer to surveillance by developing a wider understanding of what is meant by the term by providing audiences with examples of surveillance technologies, such as cameras and biometrics.

The chapter concludes with a series of recommendations for PRISMS survey. Partners have identified general recommendations to be considered in the PRISM survey: the use of clear and precise definitions of concepts, to provide respondents with neutral responses to choose from, to collect demographic information, to expand the operationalization of key concepts and to use follow-up questions. In addition, partners also identified a set of eight hypotheses (as well as examples of questions) to be considered in the development of the PRISMS survey:

1. Demographic variables have an impact on public perceptions of privacy, trust, security and surveillance.
2. People have different levels of concern about different types of privacy.
3. Different explanations are important to people in determining their acceptance of encroachments upon their privacy.
4. Citizens only take some measures of which they are aware to protect their privacy.
5. Citizens have different levels of trust in different organisations' abilities or willingness to ensure their different types of privacy.
6. Citizens hold different levels of concern over different types of security.

7. Citizens are more concerned about the impact of some surveillance technologies on their privacy than others.
8. Consists of three parts:
    a. Citizens have different beliefs in the ability of different types of surveillance technologies to enhance security.
    b. Citizens are concerned about different types of surveillance technologies and their impact on their privacy.
    c. Citizens have different levels of trust in an authority's abilities to protect their privacy when using surveillance technologies to enhance security.

Chapter 9: Conclusion: Summary of recommendations

The report concludes in chapter nine with a summary of recommendations to be considered in the development of the PRISMS survey. This summary is based on all previous findings identified within this report.

Chapter 1: Introduction

Hayley Watson, David Wright and Rachel Finn
Trilateral Research & Consulting, LLP

1 INTRODUCTION

Understanding citizens' construction of the trade-off between privacy and security requires an examination of how privacy, security, trust and surveillance are understood by members of the public in Europe and elsewhere. Although policy documents, academic literature and mainstream media materials offer some definitions of each of these concepts, there is often little connection between the way that professionals in each of these fields and members of the public understand these concepts.

Academics have found that the concept of privacy is notoriously difficult to define. Privacy is widely understood to be a social value and a public good as well as an individual value.[1] Although a widely accepted definition of privacy remains elusive, many academics have argued that privacy comprises multiple dimensions. For example, Solove asserts that privacy is best understood as a "family of different yet related things"[2]. Roger Clarke outlined, in 1997, a taxonomy of privacy that includes four different types of privacy: privacy of the person, privacy of personal data, privacy of personal behaviour and privacy of personal communication.[3] More than a decade later, Finn, Wright and Friedewald updated Clarke's categories to include seven types of privacy, including privacy of the person, privacy of behaviour and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space and privacy of association (including group privacy).[4] However, others have argued that the complexity of privacy as a concept has legal and ethical benefits. The European Court of Human Rights (ECtHR) has ruled that it is neither possible nor necessary to determine the content of privacy in an exhaustive way.[5] Furthermore, maintaining flexibility in a conceptualisation of privacy could ensure that a wide range of issues such as integrity, access to information and public documents, secrecy of correspondence and communication, protection of the domicile, protection of personal data, wiretapping, gender, health, identity, sexual orientation, protection against environmental nuisances and so on are covered by the law.[6]

However, in a policy context, the focus is on protection of personal data more than on the protection of privacy. The first European Directive related to privacy was the 1995 Data Protection Directive (95/46/EC) that is focused on organisations that process personal data. In the past few years, an intense process of stakeholder consultation has led to a recently published Proposal for a Regulation to update the existing regulatory framework.[7] This

[1] See Gutwirth, Serge, *Privacy and the Information Age*, Rowman & Littlefield, Lanham, MA, 2002; Bennett,
[2] Solove, 2008 p. 9.
[3] Clarke, Roger, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", Xamax Consultancy, Aug 1997. http://www.rogerclarke.com/DV/Intro.html
[4] Finn, Rachel L., David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Yves Poullet et al. (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, pp. 3-32.
[5] *Niemietz vs. Germany* and *Pretty vs. UK,* Judgment of 16 December 1992, § 29: "The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life'. However, it would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude there from entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings."
[6] See Gutwirth, 2002 and Sudre, Frédéric, Jean-Pierre Marguénaud, Joël Andriantsimbazovina et al., *Les grands arrêts la Cour Européenne des Droits de l'Homme*, Presses Universitaires Française, Paris, 2003.
[7] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", COM(2012) 11 final, Brussels, 25 January 2012. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

document foregrounds privacy elements such as supporting "privacy by design" technologies that integrate privacy features throughout the entire development process of a system from its earliest conception, and mandating that organisations appoint data protection officers and implement "data protection impact assessments". Developments in the ICT environment (and in particular FETs, Future and Emerging Technologies) have created new practices that threaten the privacy of individuals without actually processing their personal data. Indeed, when using the various ICTs, individuals leave a vast number of electronic traces (e.g., IP addresses) that are not personal data in the sense of the relevant directives, but which nonetheless become the resources of extensive profiling activities that entail several risks for the privacy of the persons concerned.[8] Therefore, the equation of privacy with data protection does not adequately address infringements that are not directly linked to the processing of personal data. (In any event, the Charter of Fundamental Rights of the European Union 2000 treats them separately in Articles 7 and 8 respectively.) In the context of analysing existing surveys relating to public perceptions of privacy, we will examine whether surveys predominantly focus on data protection in reference to privacy, or whether they examine various types of privacy as set out by Finn et al.[9]

Individuals in the European Union also have a right to security, and like privacy, there have also been difficulties in defining security. Zedner has argued that security is often defined as the absence or mitigation of threats, thus it depends on these very threats in order to have conceptual clarity.[10] Other researchers, such as David Brooks, argue that the "multidimensional nature of security results in both a society and industry that has no clear understanding of a definition for the concept of security. Moreover the current concepts of security are so broad as to be impracticable."[11] Given this difficulty, it is not surprising that different European languages have different words and different connotations for the meaning of security. In English, words such as security, safety and continuity are used for different aspects of being and feeling secure.[12] The German word *Sicherheit* refers to both security and safety while the Dutch and French use a different word for each (*veiligheid* and *zekerheid*, *sécurité* and *sûreté*). Furthermore, security is applied to a range of different contexts, from social security to technologically secure systems. Cyber and information security is a distinct branch which refers to secure handling of information, preventing unauthorised access and use of data. Secure communications are communications which function as expected and which are robust and vital, able to resist attacks on their functionality. Within the policy context of the European Union, security relates to the integrity of the European Union as a whole, the protection of its outer borders and the fight against criminality, terrorism, fraud and illegal immigration. Given this complex security landscape, Lagazio has argued, as mentioned above, that there are seven different types of security: physical, political, socio-economic, cultural, environmental, radical-uncertainty and cyber and information security.[13]

However, the right to privacy is often linked with an individual's right to security, as security measures often involve the increased use of surveillance technologies that have significant privacy implications. Over the past decade, the Tampere programme (1999-2004), the Hague

[8] De Hert, Paul, and Serge Gutwirth, "Regulating Profiling in a Democratic Constitutional State", in Mireille Hildebrandtand Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008, pp. 271-291.
[9] Finn et al., 2012.
[10] Zedner, Lucia, *Security*, Routledge, London, 2009.
[11] Brooks, David J., "What is security: Definition through knowledge categorization", *Security Journal*, Vol. 23, No. 3, 2009, pp. 225-239. http://www.palgrave-journals.com/doifinder/10.1057/sj.2008.18
[12] Bauman, Zygmunt, *In Search of Politics*, Polity Press, Cambridge, 1999.
[13] Lagazio, M. *Report on research approaches and results,* ETTIS project, Deliverable 2.2, 31 June 2012.

programme (2005-2009) and most recently the Stockholm programme (2010-2014) form the basis of the internal security strategy of the Commission, and deal with the protection of individual rights, the fight against terrorism, criminality, immigration and fraud. Various events (the attack on the World Trade Centre in New York, the bombings in Madrid and London) contributed to the request for new measures to safeguard Europe and its Member States from terrorist attacks and opened the door to a variety of measures which were potentially intrusive on personal privacy (such as visual surveillance, location determination, communication monitoring, biometric identification, dataveillance and sensor technologies[14]). For example, in its 2010 Communication, the European Commission presents an overview of European initiatives to safeguard the security of its citizens by combating criminal and terrorist behaviour and fighting illegal immigration.[15] It identifies 18 different initiatives some of which were established several years ago (e.g., the Schengen Information System) and some are the result of the heightened threat alerts in recent years. Furthermore, the European Security Research Advisory Board (ESRAB) has stated that more security is only possible at the price of collecting more information and increased surveillance which immediately raises questions of privacy and data protection.[16]

However, neither the Commission nor its various agencies provide any information about the acceptance of these systems by European citizens and the trust citizens' place in these surveillance initiatives for improving their security. This is surprising given the Commission's ambition to search for implementation of its security strategy while maintaining a high level of trust by citizens in its activities, by safeguarding individual rights and protecting personal data.[17] This report on existing surveys seeks to understand the position of the public in this complex relationship between privacy, security, surveillance and trust. It consists of a series of preparatory activities to be taken into consideration in the development of the PRISMS survey. Preparatory activities include: an analysis of existing surveys that focused on exploring public opinion towards privacy, surveillance, security and trust (Task 7.1), an analysis of existing surveys focusing on the methodologies employed (Task 7.2), the operationalisation of concepts and recommended hypothesis/questions (Task 7.3), lessons learned (Task 7.4) and an analysis of social value surveys and the consideration of values to be included in the PRISMS survey (Task 7.5). Accordingly, this report has the following structure.

1.1 REPORT STRUCTURE

[14] Gutwirth, Serge, Rocco Bellanova, Michael Friedewald, Dara Hallinan, David Wright, Paul McCarthy, Julien Jeandesboz, Emilio Mordini, Silvia Venier, Marc Langheinrich, and Vlad Coroama, "Smart Surveillance - State of the Art Report", Deliverable 1, SAPIENT Project, January 2012.

[15] European Commission, "Overview of information management in the area of freedom, security and justice", COM(2010) 385 final, Brussels, 2010.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0385:FIN:EN:PDF

[16] ESRAB (European Security Research Advisory Board), "Meeting the challenge: the European Security Research Agenda. A report from the European Security Research Advisory Board", Office for Official Publications of the European Communities, Luxembourg, 2006.
http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf

[17] See European Council, The Stockholm Programme – An open and secure Europe serving and protecting the citizens, 17024/09, Brussels, 2 Dec 2009 and European Commission, "An area of freedom, security and justice serving the citizen", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, COM(2009) 262 final, Brussels, 2009.

Chapter two involves an examination regarding the data collection process for the analysis of existing public opinion surveys assessed in chapters three, four and five. The chapter provides a meta-analysis of the collection of surveys, providing details as to the number of surveys, the subject area, who conducted the survey, who the surveys were conducted for, information regarding the sample size and the methodologies employed to conduct the surveys. The chapter then goes on to provide information regarding the methodology and smaller sample of surveys identified for use within the comparative analysis of existing surveys in chapter four.

Chapter three of this report provides a meta-analysis of the methodologies used in those surveys analysed for Task 7.1 (chapter four and five of this report). It aims to take stock of existing surveys at the intersection of surveillance and privacy, to consider them from a methodological standpoint of good practice, to evaluate their reliability and comparability, and to draw lessons from this exercise. The chapter concludes with a series of recommendations regarding methodological considerations for conducting the PRISMS survey.

Chapter four involves a presentation of the results of a comparative in-depth analysis of 20 existing surveys. It provides an analysis of each of the 20 surveys selected by the consortium for comparative analysis. The examination of each survey includes an introduction, an explanation of the survey's methodology, a summary of the main findings gleaned from each survey, an insight into how the survey compares to other surveys, paying close attention to any points of convergence or divergence and finally an identification of where the results of the survey may have been used elsewhere.

Drawing on the results of chapter four, chapter five consists of a horizontal analysis of each issue being explored: privacy, trust, security and surveillance. The chapter highlights the main findings unearthed in relation to public perceptions of these issues. Chapter five also provides a critique of surveys by examining the various types of privacy, trust, security and surveillance with which they deal, thereby identifying gaps in the investigation of public perceptions. Finally chapter five outlines insights gathered from socio-demographic trends, temporal changes and continuances, and any technological differences.

In chapter six partners note extraneous and situational factors that may influence responses, including media portrayals, cultural differences, knowledge of privacy laws and specific events. These considerations are then used to provide a series of hypotheses to be taken into consideration in the development of the PRISMS survey.

Chapter seven focuses on presenting an analysis of social values surveys. The chapter provides an introduction to the concept of values and charts its development within the social sciences. Chapter seven then goes on to mapping European differences in terms of cultural values based on three types of social value surveys: the World Values Survey, the European Values Survey and the European Social Survey. Finally, in support of the development of the PRISMS survey, chapter seven makes use of an exploratory approach to analyse what these values surveys suggest about the importance of cultural values in influencing public perceptions of privacy, security and related concepts. The chapter concludes with a series of potential hypotheses to be considered in the development of the PRISMS survey.

Drawing on the results of Task 7.1 (chapter four and five of this report), chapter eight provides a review and analysis of survey question techniques to support the construction of the PRISMS survey. It begins by drawing on the analysis of section two to show how existing

surveys operationalise key concepts in this analysis: privacy, trust, security and surveillance. It then goes on to propose a set of hypotheses and related questions that could be used in the PRISMS survey.

The report concludes in chapter nine with a summary of recommendations to be considered in the development of the PRISMS survey.

Chapter 2: Analysis of existing public opinion surveys: Methodology

Iván Székely
Eötvös Károly Policy Institute

Hayley Watson, David Wright and Rachel Finn
Trilateral Research & Consulting, LLP

2 ANALYSIS OF EXISTING PUBLIC OPINION SURVEYS: METHODOLOGY

In order to conduct an analysis of existing surveys to help inform the construction of the PRISMS survey, the partners drew on an external research activity that they had been involved in which involved the development of a database of existing surveys. These inter-connecting initiatives were paramount to the successful completion of tasks 7.1 through to 7.4 and will be discussed below; focusing on the nature of the data, as well as the methodology employed for the analysis of existing surveys (reported in chapter four).

2.1 DATA COLLECTION AND REVIEW

During the research into identifying and analysing existing public opinion surveys – some partners were involved in a research activity that started prior to the launch of the PRISMS project.[18] We compiled an inventory of about 260 surveys at the intersection of privacy and security/trust/surveillance, of professional and/or political importance. The date span of the inventory ranges from 1985 to early 2012. This stock of surveys formed the basis of selecting and analysing the 20 chosen surveys as presented in D7.1 (Chapter 3). However, the stock of surveys as a whole is suitable for a different kind of analysis: for identifying certain trends and patterns in the practice of creating and using surveys in the subject area of our research.

In the preliminary phase of the research we described and categorized the surveys according to 24 aspects and/or variables[19] in order to create raw material for subsequent research. Later we narrowed down the inventory to 216 surveys, leaving out unreliable or unavailable surveys, or non-surveys,[20] and this resulting stock forms the basis of the following analysis.

It is important to note that this pool of public opinion surveys cannot be regarded as a full inventory of surveys in our subject area, nor a kind of representative sample of such surveys at the global level, therefore our inventory cannot be analysed as a *statistical* sample. Since the common language of the researchers working in this task, and also the official language of the PRISMS project, is English, our inventory consists of predominantly English language surveys/publications which are publicly available. Consequently it does not include French, Dutch or even Chinese surveys, unless there exists a detailed and informative enough publication in English about the survey concerned.

Despite all the above limitations, the inventory cannot be regarded as an arbitrary list of surveys or a simple search engine hit list. The inventory had been compiled by experts whose knowledge, experience and evaluation are reflected in the compilation, as well as in creating the description and categorization of the surveys. Therefore the inventory of surveys is suitable for demonstrating certain trends during the date span of the surveys collected, and for

[18] The original initiative was suggested in one of the working groups of the LiSS (Living in Surveillance Societies) COST Action, www.liss-cost.eu

[19] Among others, the subject area of the survey, the name and type of the organization which conducted the survey, the client who commissioned the research, the scope and size of the sample, the surveying method, or – if available – the use of the survey results.

[20] For example, reports about research findings behind which there were no new empirical researches.

studying how surveys have been created and used in this area.[21] In the following we will use the information compiled about the surveys between 1985 and 2010.[22]

2.1.1 *Number of surveys*

The annual number of surveys conducted in our subject area shows an increasing trend, in line with the general trend of conducting more and more surveys during the last decades, this is partly due to the spread of new inexpensive surveying methods and tools, partly to the increasing demand of decision-makers and the media (see figure 1 below).

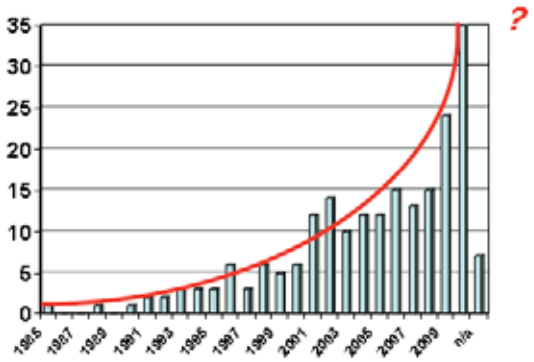


Figure 1: Number of surveys

However, the virtual red curve, seeming to rocket into an ever increasing number of surveys expected in the future, may be misleading: we can better understand the trends and discrepancies if we divide the 25-year date span into separate periods. One possible division is the following (figure 2 below): In the first period, 1985-1995, 1-3 significant surveys were conducted annually, in some years no such surveys were conducted at all, according to our criteria. In the period of 1996-2004 "in average" 5-10 such surveys could be expected annually, however, the years 2002 and 2003 show a significant increase, what we call the shockwave of 9/11 in public opinion research. Although there were surveys conducted right after the attack, only a part of these were intended to explore people's attitudes to privacy and surveillance; these research areas became popular after the introducing of anti-terrorist measures, or the enacting of the Patriot Act. Between 2005 and 2008 the annual number of surveys was 12-15, but the question is open: what would be the "normal" frequency of conducting public opinion surveys at the intersection of privacy and security/trust/surveillance in the period 2009-2010? The surprisingly high number of surveys which met our criteria (24 in 2009 and 35 in 2010) suggests us another "shockwave": the increased interest generated by the European data protection reform under way. Both supporters and opponents of the reforms may be interested in learning people's opinion and attitudes, and the decision-makers also need to take empirical research findings into consideration when developing the new regime.

[21] We will not indicate exact numbers of percentages since in this sample small differences do not have significance in statistical terms. Greater differences, or temporal shifts, however, can reveal important patterns and trends.

[22] The 2011 data are not complete, and the year 2012 is represented in the inventory by a few surveys only. In such researches there should be a state of the data set which serves as the basis for the subsequent rounds of analysis, therefore further collection of data had to be suspended or treated separately from the overall analysis.

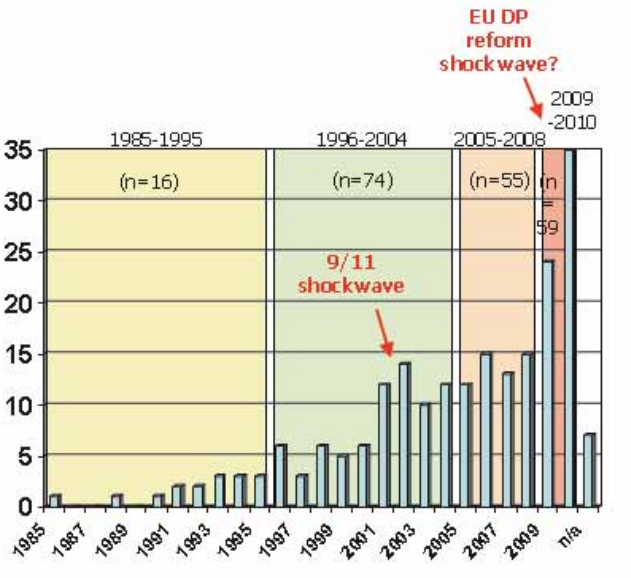


Figure 2: Number of surveys in different periods

2.1.2 *Subject area*

In one of our variables used to describe and analyse the surveys, "Subject area", we used the following categories, in an abbreviated form:

- privacy/data protection in general [PRIV/DP]
- surveillance in general [SURV]
- visual surveillance/CCTV [CCTV]
- consumers [CONSUM]
- employment [EMPL]
- health [HEALTH]
- privacy/DP law [LAW]
- dataveillance [DVEILL]
- location-based services [LBS]
- online privacy [ONLINE]
- identity [ID]
- social networks [SNS]

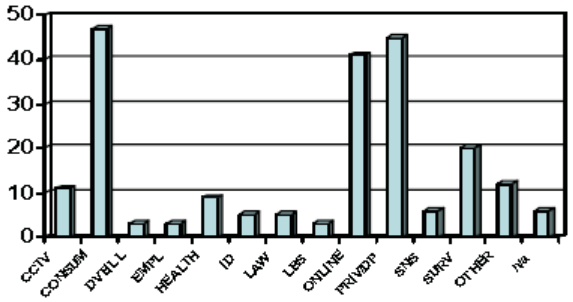


Figure 3: Subject area of surveys

Figure 3 (above) shows that the most frequent subject areas during the whole date range were consumers' privacy, privacy/data protection in general, and online privacy. Naturally, all surveys included questions relating to privacy/data protection in general, however, the surveys in our inventory had to be categorised according to the most characteristic attributes. Since a number of such categories resulted in a very low number of cases, we merged these categories into the "Other" category (Figure 4) in order to better visualise the distribution of data regarding the subject areas of the surveys.

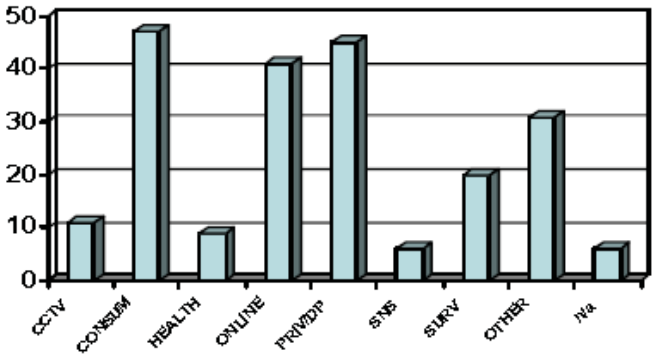


Figure 4: Subject area of surveys (merged)

If we use the same time periods we used above to demonstrate the trends in the annual number of surveys for showing the popularity of the above subject areas, we can identify certain temporal changes (Figure 5). Not surprisingly, "Online privacy" appeared in the second period only, "SNS" as a subject area of surveys appeared first in the third period, while surveys on consumers' privacy were most popular between 1996 and 2004. As to the latter, we may take risk of interpreting this figure, at least partly, as the result of the increased interest of the US industry in showing its compliance with the newly introduced data protection directive of the EU (or at least with the expectations of their consumers). Because of the differing number of surveys in the subject area categories and the differing number of surveys in the respective periods, the changing popularity of certain subject areas can be better observed on figure 6 where the overall number of surveys in the respective subject area categories is illustrated as 100%.

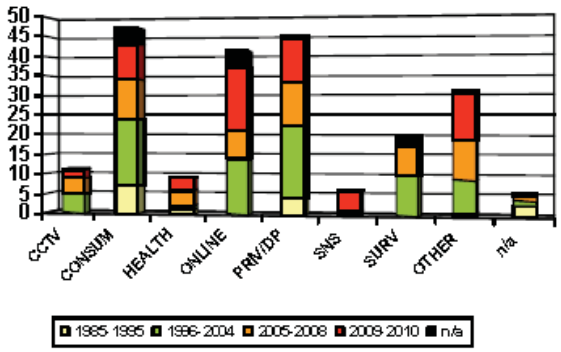


Figure 5: Subject area / periods (absolute figures)

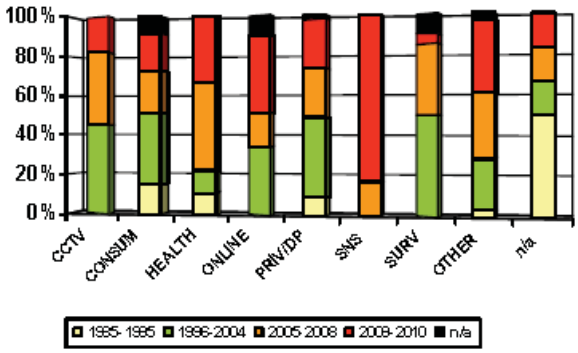


Figure 6: Subject area / periods (relative figures)

2.1.3 *Who conducted the surveys*

In the variable "Who conducted" we used the following categories:

- the Client itself [CLIENT]
- public opinion research company [PORC]
- professional organization [PROF]
- university [UNIV]
- industry [IND]
- media [MEDIA]
- civil sector organization [CSO]

According to figure 7, the majority of surveys were conducted by professional public opinion research companies; the two other important categories were the other professional

organizations and universities. This result can be regarded as a sign of quality assurance, namely that the great majority of the important surveys have been conducted by professional organizations – and this, at the same time, indirectly validates our criteria for selecting surveys for the purposes of this inventory.

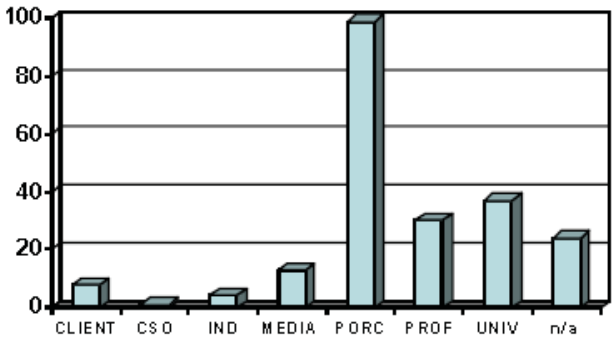


Figure 7: Who conducted the survey

It is worth noting that the "not available" category is not marginal: in more than 20 cases there was no information available on the organization which conducted the survey.

2.1.4 *The client*

The figures in the n/a category are even more striking in the case of the variable "Client", where our categories were:

- government/parliament [GOV]
- industry [IND]
- research project consortium [PROJ]
- media [MEDIA]
- university [UNIV]
- data protection authority [DPA]
- civil sector organization [CSO]
- international organization [INTL]

The chart on Figure 8 shows that in more than 80 cases there was no information published about the identity of the client – the organisation which commissioned the survey, thereby, directly or indirectly, influencing the concept of the research. Among the known categories the relatively important ones are the industry, the media, and the data protection agencies, which commissioned certain important surveys.

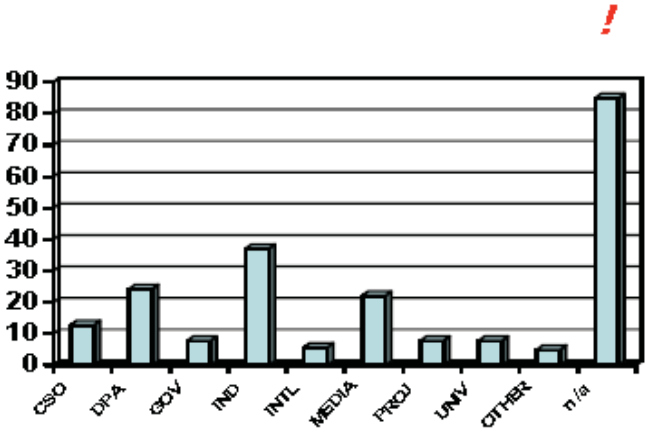


Figure 8: The client organisation

2.1.5 *Scope of surveys*

When classifying the surveys according to the scope of the surveys, we used three basic categories: cross-national, national, and sub-national. Since we regard longitudinal or comparative research an additional value, we introduced these possibilities in all the three above categories, resulting in six categories altogether. The chart on Figure 9, however, shows that our sample produced valuable figures only in four categories, of which the national and cross-national categories occupied the highest places. Here we need to note again the high number of surveys about which no information was published in this respect.

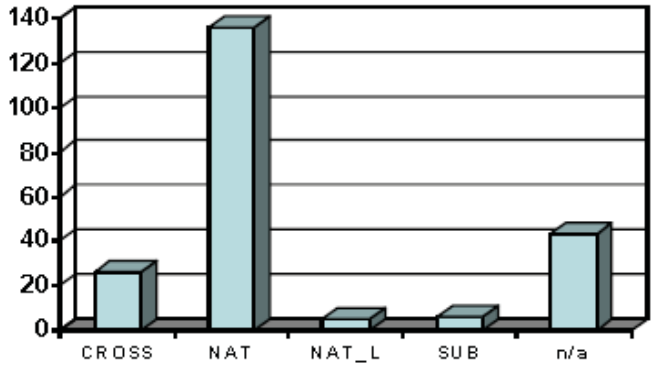


Figure 9: Scope of surveys

In Figures 10 and 11 – because of the low figures in the other categories – the only valuable information is that cross-national surveys became more popular in recent years, while there were a number of surveys of national scope conducted between 1996 and 2004.

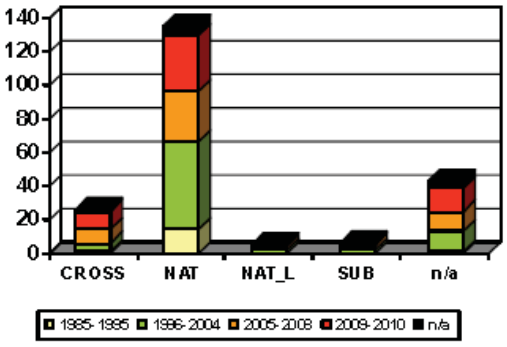


Figure 10: Scope of surveys / periods (absolute figures)

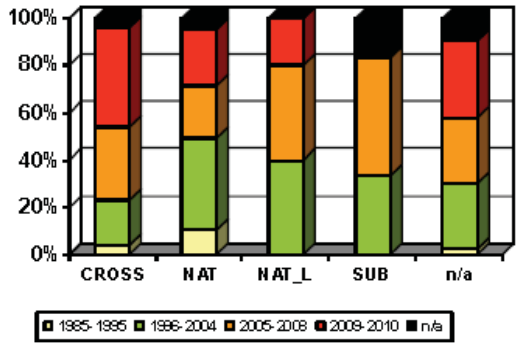


Figure 11: Scope of surveys / periods (relative figures)

2.1.6 *Characteristics of the sample*

Besides territorial scope, we classified the surveys according to the characteristics of the survey sample, whether the sample was representative in certain sense or covered a special section of the population. Our list was:

- representative/general population [REPGEN]
- representative/specific population [REPSPEC]
- age groups [AGE]
- gender groups [GENDER]
- other demographic groups [OTHGRP]
- professional groups [PROFGRP]
- internet users [IUSERS]

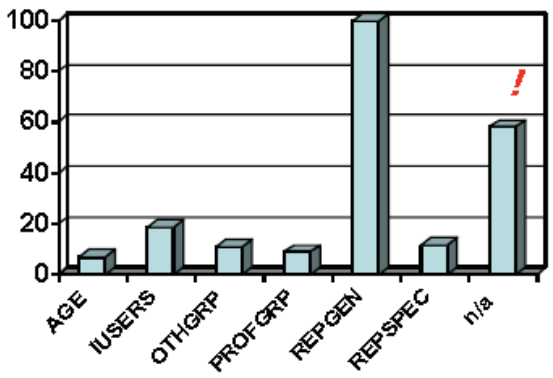


Figure 12: Characteristics of the sample

We regarded internet users as a non-representative category, although many recent surveys are conducted online, targeting internet users, as a modern equivalent of the whole population. Despite increasing internet penetration, we think that the community of internet users is not equal to the whole society, especially in certain countries, in older age groups and rural environment. Figure 12 (above) shows that the most widely used sample category was the general representative sample.[23] The number or surveys the available information about which does not contain data on the representatively or other characteristics of the sample is striking again.

2.1.7 *Sample size*

In media news and articles or in the summary reports on the surveys information about the number of respondents is more often included than other characteristics of the sample. We used the following categories for defining sample size:

- <100 [A]
- 100–1000 [B]
- 1001–3000 [C]
- 3001–10.000 [D]
- 10.001–100.000 [E]
- >100.000 [F]

Figure 13 illustrates that during the whole date range of the inventory of surveys the most popular sample size was the 1001–3000 category, representing the half of the surveys in the inventory. In this category a significant number of surveys used a sample of 1001–1010

[23] For example, a sample representing the population of a country over 18 years of age, in terms of some demographic variables such as gender, age and level of education.

respondents, just above thousand respondents, where the statistical error can already be considered low enough.

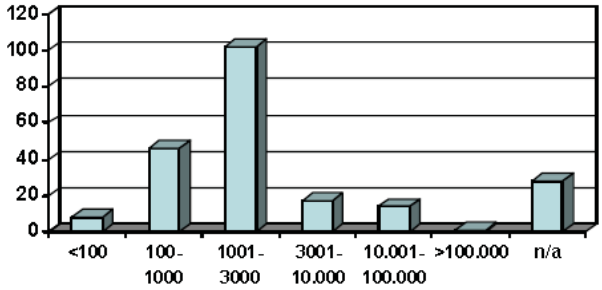


Figure 13: Sample size

Figures 14 and 15 (below) show that surveys of 3001–10.000 respondents became more frequent in the last years, supposedly in connection with the growing number of cross-national surveys, while the 1001–3000 category was most popular in the 1996-2004 period.[24]

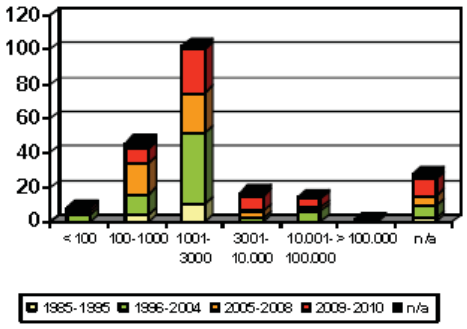


Figure 14: Sample size / periods (absolute figures)

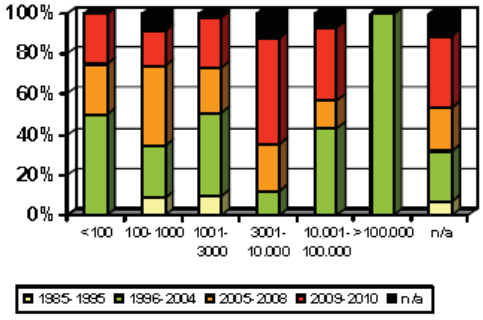


Figure 15: Sample size / periods (relative figures)

2.1.8 *Survey method*

Regarding the surveying method applied in the surveys of our inventory, initially we set up the following list of categories:

- face-to-face interviews [F2F_INT]
- face-to-face questionnaire [F2F_Q]
- face-to-face questionnaire with additional interviews [F2F_Q+]
- postal or print media questionnaire [PRINT_Q]
- online questionnaire [email, web] [ONLINE]
- online questionnaire with additional interviews [ONLINE+]
- telephone interviews/questionnaire [TEL]
- telephone interviews/questionnaire with additional interviews [TEL+]
- analysis of existing data sets [DATA]

As can be seen in the list (above), we used additional categories, similarly to the scope of surveys, expressing our view that additional interviews indicate a higher quality in survey methodology. In practice, however, it was difficult to distinguish those surveys where such

[24] There was only one survey using a sample of more than 100.000 respondents in our inventory: a Swedish survey on health privacy reaching 1,14 million citizens in a register based cancer study in 1999.

interviews had a significant role, and in several cases these additional methods were not mentioned at all in the survey reports. The result can be seen in Figure 16.

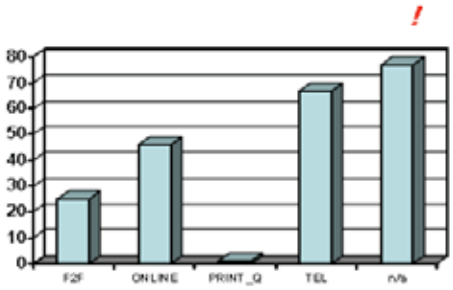


Figure 16: Survey methods

Again using our time periods, we can observe that there are differences in the popularity of certain survey methods in the subsequent periods (Figures 17 and 18): online surveys – understandably – first emerged in the period of 1996-2004, and retained their popularity in the subsequent years, and this is the period when the most telephone surveys were conducted. The only postal survey in our inventory was conducted in 2003.

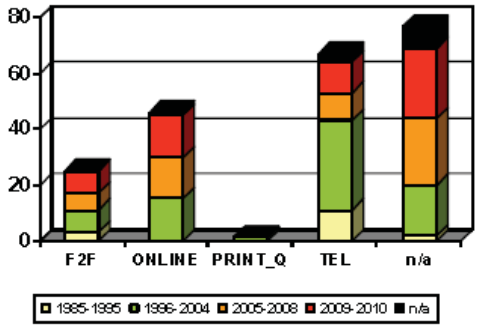


Figure 17: Survey methods / periods (absolute figures)

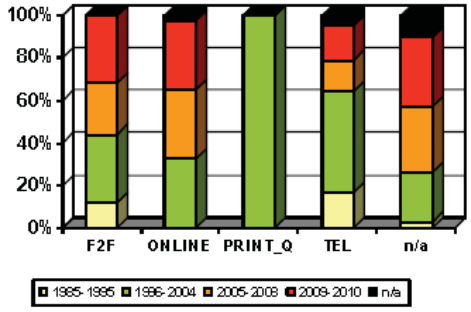


Figure 18: Survey methods / periods (relative figures)

2.1.9 *Some lessons learned*

The above analysis shows that even a non-statistical sample of public opinion surveys can be suitable for revealing important patterns and trends. The result of such an analysis may be useful both for the conceptualisation of the planned PRISMS survey and for conducting of further meta-level research into the factors behind, and the process of, creating public opinion surveys at the intersection of privacy and security/trust/surveillance, as well as the resulting findings and their use.

Within the general trend of conducting ever more surveys, we identified two "shock-waves", which indicate an increased interest in conducting public opinion surveys in our area of research: the first one after the 9/11 attack, and the second one during the preparatory phase of the European data protection reform. We used four time periods in order to present temporal changes in the characteristics of the surveys. Such changes can be seen, among others, in the popularity of certain subject areas, which we can attribute to large scale policy changes, besides the spread of new technologies and applications with strong privacy implications.

While the name and professional credits of those organisations which conducted the surveys are in most cases publicly available, the identity of the client is much less so. Similarly,

important information is missing in a significant number of surveys about the characteristics of the sample of respondents, as well as about the surveying methods. These findings reinforce our preliminary hypothesis, namely that the partial results of the surveys, which are publicised by various stakeholders and used selectively to support their interest, may not only be inherently biased but also opaque from the methodological point of view.

As a short term research aim, we need to avoid such flaws when planning and conducting the PRISMS survey; for the longer term, we need to further explore the effects of interests and agents, as well as their interdependence in creating and using public opinion surveys in our research area.

2.2 METHODOLOGY: IN-DEPTH ANALYSIS OF EXISTING SURVEYS

The selection of surveys described above, have been used to complete Task 7.1 (chapter four of this report), an in-depth comparative analysis of existing surveys. Following collection, the consortium processed and narrowed down the full set to 20 surveys for closer, comparative analysis. The consortium selected surveys using the following criteria: topic, date range, sample size, sample location and language (English only for research purposes). Within the analysis presented here, where possible, partners included examples of questions in order to assist them in constructing their own questions for the PRISMS survey. In addition, the consortium included descriptions of the survey's methodology to assist them in designing the PRISMS survey. The surveys included in this report range in date from 1997 through to 2012 allowing for a temporal analysis of results. The report highlights instances of converging and diverging opinions; for instance, there are those who claim they are concerned about their privacy, but do not take action to enhance their privacy online.

Accordingly, the analysis provided here is limited to areas of consideration relevant to PRISMS. The surveys selected provide interesting insights into both public attitudes and public behaviour regarding their attitudes towards matters relating to (for instance): consumer behaviour on the Internet, Internet usage, measures taken to enhance privacy and security on the Internet and attitudes towards surveillance technologies. For example, it includes Eurobarometer surveys that focus on European attitudes relating to public attitudes towards trusting others with managing their personal data. In addition, the report assesses surveys by PEW Internet & American Life that aim to understand Americans' digital footprints on the Internet and what this may mean for their online reputations. This analysis of surveys also includes surveys carried out by market research organisations such as Harris International, that investigate public attitudes towards increasing surveillance measures such as full body scanners to improve airport security. Surveys also stem from academic institutions, such as England's London School of Economics (LSE) study that investigates children's use of the Internet. Although some surveys may have included additional information and areas of consideration, this analysis is limited to focusing on insights that are useful for PRISMS. The authors have included additional surveys (where appropriate) from the data set to which it was interesting to refer for points of convergence and divergence across surveys. The surveys selected for in-depth analysis were spread across four conceptual fields: privacy, security, surveillance and trust. The following table (Table 1) provides a breakdown of how the selected surveys were spread across these fields:

Table 1: PRISMS - Surveys selected for in-depth analysis

Section	Title	Short title	Year	Institution	Subject area	Sample	Sample size	Field(s)
4.1	*Information technology and data privacy*	Eurobarometer 46.1: Information technology and privacy	1997	INRA (Europe)	Information technology and concern over protecting their personal data	15 EU Member States	16,246	Privacy Trust
4.2	*Support for some stronger surveillance and law enforcement measures continues while support for others declines*	Special 9/11 Poll	2002	Harris Interactive	Surveillance, terrorism	USA	2,203	Privacy Security Surveillance
4.3	*A two-edged sword – public attitudes towards video surveillance in Helsinki*	A two-edged sword: video surveillance in Helsinki	2003	The City of Helsinki Urban Facts	Attitudes towards video surveillance	Finland, Helsinki	1,240	Privacy (indirectly) Security Surveillance
4.4	*CCTV in Europe*	URBANEYE: CCTV in Europe	2004	Technical University Berlin	Attitudes to CCTV/ Surveillance	7 EU countries	1,001	Privacy Security Surveillance Trust
4.5	*e-Identity: European attitudes towards biometrics*	e-Identity: attitudes towards biometrics	2006	LogicaCMG	Consumer attitudes towards the introduction of biometric technology in the EU	7 EU countries	500	Security Surveillance
4.6	*A Survey on EU Citizens' Trust in ID Systems and Authorities*	Survey on citizens trust in ID Systems and Authorities	2007	LSE	EU citizens' perceptions and attitudes towards issues involved in making eIDs interoperable	23 EU countries	1,906	Privacy Trust

Section	Title	Short title	Year	Institution	Subject area	Sample	Sample size	Field(s)
4.7	*Digital Footprints: Online identity management and search in the age of transparency*	PEW Internet & American Life: Digital Footprints	2007	Princeton Survey Research Associates	Attitudes to personal information online and usage	USA	2,373	Privacy
4.8	*Data Protection in the European Union Citizens' perceptions Analytical Report*	Flash Eurobarometer 225: Citizens' perceptions of data protection	2008	Gallup Organization Hungary	Public's general feelings and concerns about the privacy of their personal data	27 EU Member States	27,000	Privacy Security Surveillance Trust
4.9	*Personlig Integritet: A Comparative Study of Perceptions of Privacy in Public Places in Sweden and the United States*	Personlig Integritet: Perceptions of privacy in public spaces	2008	University of Washington, Stockholm University, Seattle Pacific University	Cross-cultural study of people's judgements about privacy in public places	Sweden and USA	600	Privacy Surveillance
4.10	*Personal Data Project: An International Survey on Privacy and Surveillance*	The Globalization of Personal Data Project	2008	Queens University/ Ipsos	Opinions on surveillance	Cross-national	9,606	Privacy Security Surveillance Trust
4.11	*Canadians and Privacy*	Canadians and Privacy	2009	EKOS Research Associates Inc.	Opinions on privacy	Canada	2,028	Privacy Security Surveillance Trust
4.12	*Privacy 2.0: personal and consumer protection in the new media reality*	Privacy 2.0	2009	SINTEF	Attitudes and experience concerning consumer protection and privacy	Norway	1,372	Privacy
4.13	*State of the Nation Survey 2010*	State of the Nation	2010	ICM	Opinions on data protection/privacy	UK	2,288	Privacy Security Surveillance Trust

Section	Title	Short title	Year	Institution	Subject area	Sample	Sample size	Field(s)
4.14	*Most Adults in Largest European Countries, U.S. and China Agree Full Body Scanners Should be Introduced in Airports*	Financial Times/Harris Poll: Body scanners	2010	Harris Interactive	Opinion on body scanners	Cross-national	7,256	Security Surveillance
4.15	*Unisys Security Index*	Unisys Security Index	2010	UNISYS	Opinions on a range of security issues and body scanners	EU	10,000	Privacy Security Surveillance
4.16	*Reputation Management and Social Media. How people monitor their identity and search for others online.*	PEW - Reputation Management	2010	Princeton Survey Research Associates International	Internet usage and privacy management	USA	2,253	Privacy Trust
4.17	*Examining the Safety of Children Online Across Europe*	EU Kids Online: Risks and Safety on the Internet	2010	Ipsos MORI	Online risks – children's perspectives	25 EU countries	23,420	Privacy Security
4.18	*Attitudes on Data Protection and Electronic Identity in the European Union*	Special Eurobarometer 359: Data protection and e-Identity	2011	TNS Opinion & Social	Awareness of and attitudes on disclosure of personal data, profiling, identity management	27 EU Member States	26,574	Privacy Security Surveillance Trust
4.19	*Less than Half of People Surveyed Think About How Their Online Activities Impact Their Online Reputations*	Online Profile & Reputation Perceptions Study	2011	Blueocean market intelligence & Telecommunications Research Group	Online privacy, online reputation	Cross-national	5,000	Privacy Security

Section	Title	Short title	Year	Institution	Subject area	Sample	Sample size	Field(s)
4.20	*Internet Privacy Research*	Internet Privacy Research	2012	University of Queensland Centre for Critical and Cultural Studies	Explores Australian communities' understanding of and attitudes towards online privacy	Australia	965	Privacy

Chapter 3: Meta-analysis

Charles D. Raab
The University of Edinburgh

3 META-ANALYSIS

3.1 INTRODUCTION: SURVEYS AND THEIR USE

Over the past 40 years there have been a large number of public opinion surveys of attitudes towards, or knowledge about, surveillance and privacy, including visual surveillance, collection and processing of personal data, online monitoring, and the tracking of mobility. In addition to commercially based surveyors, academics specialising in surveillance studies and related fields are involved as the producers of surveys, or as users of surveys in their own research. Researchers, policy-makers, regulators and the general public are often presented with findings and conclusions of these surveys. The methods used are often flawed, and the findings and conclusions are often biased, yet these are interpreted and used selectively by participants in the process of policy-making to support their different causes. The media as well as various interests – privacy NGOs, business, governments, etc. – like to point to surveys that support their interest or cause, and to ignore other ones that lean in a different direction: there is a tendency selectively to "cherry-pick" the findings one likes. This contributes to the distortion of debate and policy-making concerning surveillance.

A main concern of work package seven (WP7) is that the limitations of individual surveys are often overshadowed by headlines that can mask reasons for caution in considering the findings. Inferences about the state of public opinion as "revealed" in some surveys may be erroneous, thus distorting knowledge and – perhaps of greater importance – lending unwarranted support for certain policies. Given that many, if not most, surveys are sponsored and designed with policy relevance and influence foremost in mind, it is crucial that their vulnerability on methodological grounds be reduced, regardless of where their users and sponsors lie on the spectrum of opinion and policy concerning privacy, surveillance, and related issues. A UK House of Lords Select Committee report observed that "[r]esearch commissioned or conducted by government, business and the media cannot always be taken as disinterested. Assertions about what 'the public' feel or want concerning surveillance are not conclusive, although they often go unchallenged." The Committee called for an examination of "ways of improving the independent gathering of public opinion on a range of issues related to surveillance and data processing."[25] WP7 may be seen as a step in that direction.

Although it is recognised that surveys in this field are very difficult to conduct and to interpret, the question of survey reliability and comparability across time, space and domain is often put on one side. This is unsatisfactory, and it is important to take stock of existing surveys, to analyse them from a methodological standpoint of good practice, and to evaluate their reliability and comparability. It is also important to draw lessons so that surveys in the future can be conducted and reported on a better footing. There has been very little, if any, effort towards an independent "survey of the surveys" covering the life-cycle of such surveys, from the conceptualisation of the research through drafting the questionnaire, selecting the sample and methodology, to the interpretation, citing and use of the results. This lack of critical awareness about privacy survey methodology impedes knowledge and understanding of surveillance and its perceived effects. As Haggerty and Gazso show, it has serious political

[25] House of Lords, Select Committee on the Constitution, 2nd Report of Session 2008-09, *Surveillance: Citizens and the Tate*, Volume I: Report, HL Paper 18-I, paras. 399, 400. Charles Raab, one of the contributors to this Task, was the Specialist Adviser to the Select Committee for this Report.

consequences.[26] Gandy agrees, illustrating the point with examples of the shaping of US policy-making through interested parties' strategic use of surveys on privacy attitudes, and citing literature that emphasises that "[o]pinion polls influence policy formation by what they measure and report, as well as by what they ignore…The fact that a particular question is asked may add legitimacy to a policy option that might otherwise not be considered.".[27]

WP7 aims to help redress this situation, using a "survey of selected surveys" and the discussion of their findings to focus upon the various specific methodologies used in carrying out surveys relating to surveillance and privacy. It notes features such as survey subject, location, date, type of population sampled, sample size, response rate, and the method of administering the survey. It takes account of the elements and process(es) of creating the surveys, from the expectations of the client through the methodology chosen for the collection, interpretation and dissemination of the results. The aim is an overview of existing surveys at the intersection of surveillance and privacy, considering them from a methodological standpoint of good practice, evaluating their reliability and comparability, and drawing lessons from this exercise.

One of the key questions is whether and how the methodology used to carry out public opinion surveys may influence the outcome of the survey. Attention should be paid to variations in sample size, sampling strategy, response rate, the wording of questions, and other sources of possible bias. This permits an assessment of the quality of surveys, enabling PRISMS to be better aware of methodological considerations for conducting its own survey. The present Task limits itself to observations on only a few issues that are manifest in many surveys in this field, with reference to the small sample analysed in this WP that have prompted these observations. Attention is focused upon response rates, reporting response rates, displaying the questionnaire, the consistency of reporting of demographic variables across surveys, and problems in cross-national or cross-cultural surveys.

3.1.1 *Recapitulation*

It would go far beyond the feasible scope of WP7 to analyse in depth the entire data set of 260 surveys mentioned in chapter two (Task 7.1). Table 1 of Chapter two displayed the characteristics of the 20 surveys that were selected for further analysis, and the Appendix to Task 7.2 (annex 1) is a further table that gives additional information relevant to the methods used in those 20 surveys.[28] Although some surveys were not explicit or comprehensive in describing their methods, these surveys varied considerably in several ways:

- *Provenance:* Some were conducted by academic researchers, while others were produced by well-known commercial survey and research organisations.
- *Client:* some surveys were carried out for governmental bodies including the European Commission, while others were sponsored by private companies, academic organisations, or the media.

[26] Haggerty, Kevin D. and Amber Gazso, "The Public Politics of Opinion Research on Surveillance and Privacy", *Surveillance & Society*, Vol. 3, Nos. 2-3, 2005, pp. 173-180.
[27] Gandy, Oscar H., Jr, "Public Opinion Surveys and the Formation of Privacy Policy", *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 283-299, at p. 284. He cites Ginsberg, B., *The Captive Public: How Mass Opinion Promotes State Power*, Basic Books, New York, 1986.
[28] The table shown in the Appendix contains the same 20 surveys but with an altered content and format. It indicates the date of fieldwork when the survey data were recorded, and not the date of publication, and it follows strict chronological order.

- *Coverage of fields:* these ranged across privacy, identity, security, surveillance, and trust.

- *Subject focus:* these included attitudes towards video surveillance, biometrics, online data usage, social media, body scanners, government policies and laws, and profiling; one survey focused upon children's online experience; another survey was conducted within a few months of the "9/11" attacks and probed public attitudes towards law enforcement and surveillance.
- Definition and use of key concepts.[29]
- *Sample scope:* some surveys were conducted within a smaller or larger number of EU countries; others covered single countries (e.g., Finland, US, Canada, Norway, Australia) or were cross-national and comparative in their scope, either within the EU or globally; some surveys were confined to particular cities (e.g., Helsinki, Berlin, Budapest, London, Oslo, Vienna) rather than a country as a whole; all continents except Africa (no surveys) were represented by at least one country.
- *Sample size:* owing to these differences, the sizes of samples ranged from 500 to over 26,000, although if the multi-country surveys, such as those conducted in a large number of EU countries (e.g., Eurobarometer surveys), are considered in terms of the sample size in any one country – typically ± 1,000 – the range is still fairly wide.
- *Sample selection:* this varied, from approaches to people in public places, to the use of registers, to the self-inclusion of respondents, although some surveys were not clear about the method of selection.
- *Method of conducting the survey:* this included – singly or in combination – telephone interviews, face-to-face interviews, and online or other self-completion questionnaires; one survey also used preliminary focus groups.
- *Date of fieldwork:* the earliest of the 20 surveys was conducted in late 1996, and the most recent in late 2011; the dates were fairly evenly spread across the years but with particular concentrations in 2006 and 2010; as mentioned, one survey was conducted not long after the events of 11 September 2001.
- *Achieved sample:* this was in many cases weighted in various ways to reflect population demographics in terms of gender, age, and other variables; although no survey could claim to be random, many were regarded as "representative", although the method of conducting a survey – e.g., by telephone – will have inevitably introduced an element of bias. We discuss a further and major source of bias in the next section.

3.1.2 *Problems of method and reporting*

It would be possible cautiously to make some comparisons and generalisations about people's attitudes, as Task 7.1 will show (chapter four). However, the differences among surveys in terms of the methodological aspects mentioned above, along with variations in the wording of questions, in the indication of context in questionnaire items, and in other aspects of method will have a strong bearing on the validity and comparability of the substantive findings about what people think of privacy, surveillance, or other topics. Dillman states that

> [a] good sample survey, by whatever method [mail, telephone, face-to-face], is one in which all members of a population have a known opportunity to be sampled for inclusion in the

[29] Deeper analysis of the questions asked and of how the fields and subjects have been operationalised in surveys can be found in Tasks 7.1 and 7.3 (chapters 4, 5, 6 and 8 of this report).

> survey (non-coverage error is avoided); the people to be surveyed are sampled by random methods in sufficiently large numbers to provide a desired level of precision (sampling survey error is limited); questions are selected and phrased in ways that result in people providing accurate information (measurement error is avoided); and everyone who is included in the sample responds (nonresponse error is avoided). Seldom if ever does a sample survey accomplish all of these goals. However, this multifaceted concern becomes a standard by which progress in the development of mail survey methods can be measured.[30]

Surveys in the field of privacy and surveillance would be especially hard put to achieve this ideal, and it is unrealistic to expect these "errors" to be avoided. That said, we believe that the surveys discussed here fall prey to some, if not all, of these defects, such that conclusions about the state of public opinion must be hedged about with *caveats*. The PRISMS survey should not be expected to have achieved the ideal, owing to how it was conducted and other features of its methods as well. It is based on quota samples that "represent" the populations from which they are drawn, and does not purport to be a random sample. This does not vitiate its findings or any discussion that might follow from them, and in any case its methods are transparently reported so that the salience of any deviation from the "ideal" can be judged.

3.1.3 *Response rate*

We concentrate mainly on a few methodological problems of the surveys we have examined; the first is the response rate. This problem is of particular importance in surveys on privacy and surveillance that deeply affects our understanding of public attitudes on these subjects. Citing other literature,[31] Haggerty and Gazso assert that

> in few other fields does the issue of response rate have such self-evident political implications as in public opinion studies relating to issues of randomness, representativeness and thus the generalizeability [sic] of findings to the surveillance/privacy. … For our purposes we are not specifically concerned with the issue of absolute response rates… . Instead, our focus is on the randomness of the non-response. Depending on various factors relating to a survey's timing, the technology used, or the subject matter, certain classes of people will be differentially inclined to offer their voluntary consent to participate in a study... . If the factors that lead certain groups of individuals to be disproportionately excluded from a survey are in some way related to the topic being studied, then the non-response can be a major methodological limitation. Internet surveys about computer usage…disproportionately exclude the opinion of people without computers, something that is itself correlated with various demographic and attitudinal variables. In such cases the differential response can be vitally important as it calls the representativeness of the study's findings into question… . Public opinion surveys on

[30] Dillman, D., "The Design and Administration of Mail Surveys", *Annual Review of Sociology*, Vol. 17, 1991, pp. 225-249, at pp. 228-229.

[31] Groves, R.M., R.B. Cialdini and M.P. Couper, "Understanding the Decision to Participate in a Survey", *Public Opinion Quarterly*, Vol. 56, 1992, pp. 475-495; Dillman, D., "The Design and Administration of Mail Surveys" *Annual Review of Sociology*, Vol. 17, 1991, pp. 225-249. Dillman focuses on mail surveys but also compares these with telephone and face-to-face interviews, where the difficulties may be somewhat different but no less severe, and perhaps more-so.

> surveillance/privacy are an extreme instance where we can expect a degree of important non-randomness to be structured into response rates.[32]

Illustratively, these authors report that a telephone survey on attitudes towards security and civil liberties, commissioned by *The Globe and Mail* newspaper in Toronto, had a response rate of only 11.6 per cent, taking the high non-contact rate into consideration as well, thus arguably greatly under-representing pro-privacy views among those who refused contact or declined to be interviewed on this subject.[33] Some people regard surveys as intrusions on their privacy, and therefore non-responders cannot be assumed to be randomly distributed across the spectrum of attitudes to privacy. We cannot tell, overall, how far a low response rate is a flaw in the surveys under consideration in this WP, or precisely how the respondents in any survey are disproportionately structured in the way suggested by Haggerty and Gazso. As Dillman suggests, inability to know this may be an inherent problem in surveys where the population distribution of certain characteristics – in this case, attitudes to privacy, surveillance, security, etc. – cannot be known in advance and where overcoming such lack of knowledge is in fact a rationale for the survey. But it is beyond the scope of the present Task to propose ways of boosting the response rate in the PRISMS survey by means of one or more of the techniques that may be available, whether through incentives to take part in a survey, greater personalisation of approach, follow-ups, altering the length of a questionnaire, or by other means.[34] These matters, and any investigation of reasons for non-response, are best handled through the expertise of the professionals involved in conducting the PRISMS survey.

3.1.4 *Reporting response rates*

In any case, perhaps the most worrying deficiency in the reporting of the 20 surveys that have been analysed, and indeed in the very large number of surveys known to us, is the typical *failure to report* the response rate in surveys where the method of collection makes it relevant to know this item of information. Without such knowledge, it is too easy for "consumers" of surveys to forget about the necessary caution with which interpretations of findings should be approached. Among the 20, 14 did not indicate anything about the response rate. The six exceptions (two of which were from the same survey organisation) and their explanations were:

1. *A two-edged sword – public attitudes towards video surveillance in Helsinki*[35]: "A random sample of 2000 people was taken, and their address data were provided by the Finnish

[32] Haggerty and Gazso, 2005, pp. 174-175. Clarke observes: "It seems reasonable to assume that distributions of responses from people who are willing to answer questionnaires about privacy topics will be different from those that would arise if it were possible to obtain responses from those who decline to participate. Moreover, it would seem reasonable to assume that a significant proportion of those who decline do so because they place a high value on privacy. Hence there is likely to be a systematic bias in the data that is gathered, with the level of privacy concern in the population consistently under-stated by the respondent sample.", Davison, Robert M., Roger Clarke, H. Jeff Smith, Duncan Langford and Bob Kuo, "Information Privacy in a Globally Networked Society: Implications for IS Research", *Communication of the Association for Information Systems*, Vo. 12, 2003, pp. 341-365, at p. 344.

[33] Haggerty and Gazso, 2005, p. 176.

[34] Dillman, D., "The Design and Administration of Mail Surveys", *Annual Review of Sociology*, Vol. 17, 1991, pp. 225-249, at pp. 229-230. See his further discussion of meliorative techniques, pp. 230-241.

[35] Koskela, Hille, *A Two-edged Sword – Public Attitudes Towards Video Surveillance in Helsinki*, The European Group for the Study of Deviance and Social Control, Department of Geography, University of Helsinki, August 2003. http://www.europeangroup.org/conferences/2003/index.htm

Population Register Centre. We received 1,240 approved responses, which gave a response rate of 62 per cent."

2. *URBANEYE: CCTV in Europe*[36]: the percentages of premise declining to give detailed information were 87 per cent (Budapest), 72 per cent (Berlin), 55 per cent (Vienna), 27 percent (Oslo), 26 per cent (London) and 23 per cent (Copenhagen).
3. *A survey on EU Citizens' Trust in ID Systems and Authorities*[37]: "A limitation of the survey was … that the response rate from some countries was very low."
4. *PEW Internet & American Life Project: Digital Footprints*[38]: "Non-response in telephone interviews produces some known biases in survey-derived estimates because participation tends to vary for different subgroups of the population, and these subgroups are likely to vary also on questions of substantive interest. In order to compensate for these known biases, the sample data are weighted in analysis. … [Princeton Survey Research Associates] calculates a response rate as the product of three individual rates: the contact rate, the cooperation rate, and the completion rate. Of the residential numbers in the sample, 73 percent were contacted by an interviewer and 41 percent agreed to participate in the survey. Eighty-six percent were found eligible for the interview. Furthermore, 92 percent of eligible respondents completed the interview. Therefore, the final response rate is 27 percent."
5. *PEW Internet & American Life Project: Reputation Management and Social Media*[39]: see above for the general explanation of method, with the conclusion that "the response rate for the landline sample was 19.1 percent. The response rate for the cellular sample was 15.6 percent."
6. *Privacy 2.0: personal and consumer protection in the new media reality*,[40] a Norwegian two-stage longitudinal study. The 2,000 participants in the first round of the Internet e-mail survey amounted to a 71 per cent response rate, the highest of those surveys reporting this statistic. In the second round, 1,372 (69 per cent) of the 2,000 responded, a drop-out rate of 31 per cent that the authors say "is usual in long-term studies of this type". This figure – 1,372 – is the one that is used in this study to discuss the findings, but the description of the methods leaves it unclear about the administration of the questionnaire in the two stages.

3.1.5 *Displaying the questionnaire*

Just as with reporting response rates, there is evidently no "good practice" norm that enjoins surveyors to divulge the questionnaire, much less that standardises the form and manner in which it is shown. In evaluating surveys, it is important to understand the main features of the questionnaire that is used in any survey because a host of factors are considered to have a possible effect upon the answers. These factors include the length of the questionnaire, the

[36] Hempel, Leon, and Eric Topfer, *URBANEYE: CCTV in Europe*, Centre for Technology and Society, Technical University Berlin, August 2004. http://www.URBANEYE.net/results/ue_wp15.pdf

[37] Backhouse, James, and Ruth Halperin, "A Survey on EU Citizens' Trust in ID Systems and Authorities", *FIDIS Journal*, No. 1, June 2007.
http://journal.fidis.net/fileadmin/journal/issues/1-2007/Survey_on_Citizen_s_Trust.pdf

[38] Madden, Mary, Susannah Fox, Aaron Smith and Jessica Vitak, *Pew Internet & American Life Project: Digital Footprints*, Pew Internet & American Life Project, December 2007.
http://www.pewinternet.org/Reports/2007/Digital-Footprints.aspx

[39] Madden, Mary, and Aaron Smith, *Pew Internet & American Life Project: Reputation Management and Social Media. How People Monitor Their Identity and Search for Others Online*, Pew Research Center, 26 March 2010.
http://pewinternet.org/Reports/2010/Reputation-Management.aspx

[40] Brandtzaeg, Petter Bae and Markia Luders, *Privacy 2.0: Personal and Consumer Protection in the New Media Reality*, SINTEF Report, The Norwegian Consumer Council, 2 November 2009.
http://sintef.academia.edu/PetterBaeBrandtz%C3%A6g/Papers

sequence and wording of questions, the choices available for response, the show-card or other techniques used in interviewing, and others.

Unfortunately, only about half the surveys discussed earlier included their full questionnaires or made them readily available through online links. The surveys that showed full questionnaires are the three Eurobarometer surveys (but one of them shows an indistinct photocopy of the questionnaire); the Helsinki survey; the Globalisation of Personal Data survey; Canadians and Privacy; State of the Nation (although only a few questions are on privacy, surveillance or security); Financial Times/Harris (which has very few questions); Unisys (through indirect access); EU Kids Online (but elusive on the website); and the Queensland internet privacy research. A few others gave glimpses of some questions in the tables that report the findings, enabling one to see these questions or infer their wording. Several more surveys gave nothing.

3.1.6 *Consistency and reporting of demographic variables across surveys*

Opinion and attitude surveys typically report findings, and often gather their samples as well, in terms of demographic variables that include age (and age categories), gender, geographical location, level of education, and many others. Surveys in the privacy field do likewise. However, the categorisation within certain variables is not standardised: there are variations, and it is difficult to appraise their significance in terms of the reported findings. Age is a good illustration of this: only some of the 20 surveys reported in Task 7.1 (chapter four) give a clear description of the age categories used, while many others leave the reader to infer them from a scrutiny of the findings. Among those that clearly report the age breakdown:

- URBANEYE uses 15-19, 20-39, 40-59, and 60+
- Eurobarometer 46.1 and Flash Eurobarometer 225 use 15-24, 25-39, 40-54, and 55+
- Privacy 2.0 uses 15-30, 31-40, 41-50, 51-60, and 61-75.

It is not clear whether surveys choose their age categories according to hypotheses that are to be tested, although ideally there should be an explicit rationale for the selected breakdown. A similar comment would apply to geographic/cultural distinctions, as between urban and rural, east and west, north and south, or others that are typically found. Moreover, when data on such variables are cross-tabulated and reported as findings, further problems of interpretation may occur owing to the nature of the categories in each of the cross-tabulated variables. Leaving aside demographic variables, the aggregation of responses into certain categories of types of persons – the most famous being the Harris and Westin trio of privacy "fundamentalists", "pragmatists", and the "unconcerned"[41] – may be unwarranted yet politically potent in terms of shaping policy discourse through the persistence of the labels used and the characterisation of types.

The cross-national comparability of demographic variables such as income (and its distribution) or the quality and level of education cannot be assumed, as Zureik and Harling Stalker point out.[42] Beyond that, the uncertainty about why certain variables are used and broken down more finely in particular ways, the variable extent to which the basis facts about the demographic variables are reported, the substantive variations in the finer categorical

[41] Harris, Louis and Alan F. Westin, *Harris-Equifax Consumer Privacy Survey 1991*, Equifax, Atlanta, 1991.
[42] Zureik, Elia and L. Lynda Harling Stalker, "The Cross-Cultural Study of Privacy: Problems and Prospects", in Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon and Yolande E. Chan (eds.), *Surveillance, Privacy and the Globalization of Personal Data: International Comparisons*, McGill-Queen's University Press, Montreal & Kingston, 2010, p. 21.

details, all contribute to a lack of certainty about what understanding we are supposed to derive about attitudes towards privacy and surveillance on the basis of a particular survey or of a set of surveys. Elsewhere in WP7, we attempt to set out some hypotheses to guide the PRISMS survey, and we aim to provide a hypothesis-related rationale for collecting and categorising more unusual kinds of data that are not usually included in surveys in this field but that might have explanatory power in terms of the opinions and attitudes.

3.1.7 *Problems in cross-national or cross-cultural surveys*

In view of the fact that the PRISMS survey covers a large number of countries, some remarks about cross-national or cross-cultural surveys may be in order. We cannot assume that "Europe" or "the EU" constitute a homogeneous culture ranging across 27 countries, or that even within any such country there is homogeneity in attitudes towards privacy, surveillance, or security, which form the dependent variables. The Eurobarometer surveys are the nearest model, but there are other surveys that have elicited attitudes in a variety of countries. The *Globalisation of Personal Information* survey made comparisons across the US, Canada, China, Japan, Brazil, Spain, Mexico, Hungary, and France – ostensibly a wider and more varied range than a study confined to countries of the EU – and the authors' thoughtful remarks on methodology bear close attention.[43] Among other difficulties confronting empirical researchers, the meaning of "privacy" is elusive, and has long been debated by scholars even within one (Western) cultural frame of reference. Its meaning is widely variable even amongst people within single "cultures", and cannot perforce be assumed to have a universal meaning across many such cultural or national frames that would otherwise make survey questions about privacy more straightforward. Clarke points out that

> [t]he laws of most countries do not define the term "privacy", because it is so highly open-textured. It has multiple dimensions, at least those of privacy of the person, of personal behaviour, of personal communications, and of personal data… . Hence respondents may make very different interpretations of the most carefully phrased question. Yet it is unusual for researchers to provide respondents with any kind of tutorial, or even a glossary, and it is unusual to see discussions of the steps taken to overcome measurement and response bias arising from such difficulties, or to assess their impact.[44]

In addition, different countries' political histories vary greatly in terms of the populations' experience with different state propensities to interfere with privacy and to maintain extensive and intensive surveillance.

---

[43] See the thoughtful discussion in Zureik, Elia and L. Lynda Harling Stalker, "The Cross-Cultural Study of Privacy: Problems and Prospects", in Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon and Yolande E. Chan (eds.), *Surveillance, Privacy and the Globalization of Personal Data: International Comparisons*, McGill-Queen's University Press, Montreal & Kingston, 2010, pp. 8-30.

[44] Davison, Robert M., Roger Clarke, H. Jeff Smith, Duncan Langford and Bob Kuo, "Information Privacy in a Globally Networked Society: Implications for IS Research", *Communication of the Association for Information Systems*, Vo. 12, 2003, pp. 341-365, at p. 344. Zureik and Harling Stalker make a similar point; see Zureik, Elia and L. Lynda Harling Stalker, ""The Cross-Cultural Study of Privacy: Problems and Prospects", in Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon and Yolande E. Chan (eds.), *Surveillance, Privacy and the Globalization of Personal Data: International Comparisons*, McGill-Queen's University Press, Montreal & Kingston, 2010, p. 20.

3.2 CONCLUSION

Two issues have been briefly raised here: one concerns *methodological problems* in surveys on these topics. These include non-response, issues concerning demographic variables, the diverse meanings of privacy, and other shortcomings that were not examined in greater detail above. Problems in comparative research have been highlighted as well. Looking across the range of surveys, another serious shortcoming is the frequent failure to describe fully, and in some reasonably standard way, the methods used in conducting the survey, including sampling procedures. Then, too, there is the possible bias introduced by the method of data-gathering, especially online. The mitigation of these difficulties so that greater confidence can be enjoyed by those who use surveys for their political, business or other purposes is an essential requirement.

The second issue is *methodological transparency*. Surveyors are apparently reticent to report non-response rates and to show their questionnaires so that others can appraise, and learn from, the choice and manner of asking the questions, the response choices given to respondents, and other salient elements of surveying. Having this information makes it possible not only to judge the validity of results, but also to learn good (and bad) practice for the benefit of future surveys. There may be good proprietary reasons for surveyors and their organisations to be reluctant to "show the work", but such reluctance is inimical to the pursuit of other scientific values: openness, the ability to develop alternative interpretations based on the information commonly available, and the empowerment of potential critics. Moreover, in such a closely policy-relevant field as privacy, security and surveillance, it inhibits informed debate. Overcoming the lack of transparency is likely to be more easily within the control of the surveyors than the problems of method.

One of the important results of the analysis undertaken in WP7 is therefore the illumination of shortcomings and incommensurability in the surveying of opinion in the privacy field, with a view to improvement. Haggerty and Gazso urge that "scholars and advocates should publicly express their reservations…Such commentary should not be confined to academic journals, but must also be communicated to politicians, polling firms, privacy advocates, journalists, and the public at large…"[45]. On the other hand, the proliferation of surveys over several decades and across many countries does provide a rich resource for devising useful and reputable surveys that mitigate the methodological problems as far as possible and are candid about the difficulties of achieving an "ideal" instrument for ascertaining and analysing public opinion.

Building upon existing surveys, we can offer some pointers to the PRISMS survey. First, its size and range is directly comparable to the Eurobarometer surveys of privacy-related topics conducted in all the countries of the EU. Those surveys should, and will, be the natural comparators and close attention will be paid to the questions asked over the years, which are readily obtainable. Second, there are several infrequently examined dimensions that could be explored through the medium of the PRISMS survey, because we hypothesise that opinions and attitudes in this field are shaped by a number of contextual[46] and personal factors in the

[45] Haggerty and Gazso, 2005, p. 177.

[46] The importance of considering privacy in context is particularly important, and questions put to survey respondents should be designed as far as possible to tap into differences in the contexts in which the privacy of personal data is at stake in business or state information-processing activities. See Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, CA, 2010; Solove, Daniel J., *Understanding Privacy*, Harvard University Press, Cambridge, MA, 2008, pp. 47-49.

daily lives of respondents that could be interrogated, although great care is essential in devising appropriate questions to tap these dimensions. These are indicated in greater detail elsewhere in this report (e.g., see chapters six and seven).

Chapter 4: Analysis of existing public opinion surveys

Hayley Watson, David Wright and Rachel Finn
Trilateral Research & Consulting, LLP

4 ANALYSIS OF EXISTING PUBLIC OPINION SURVEYS

The PRISMS project primarily aims to understand public attitudes towards the trade-off between privacy and security and seeks to discover whether people feel that enhanced surveillance measures impede their privacy. Chapter four of this report examines public opinion surveys to explore what past surveys on privacy, trust, security and surveillance have revealed about citizens' perceptions of these issues. In addition, this analysis of surveys aims to provide an indication of what (if any) measures citizens are taking to enhance their security, their privacy and their trust in organisations that might impact upon either.

In this chapter, we present the results of an analysis of each of the 20 individual surveys we examined in detail. For ease of reference, the surveys are presented in date order, with the earliest survey examined first. For each survey, we introduce the survey, describe the methods and sampling strategy used in the survey, present the main findings (relevant to our work on PRISMS) and contextualise the survey in relation to other surveys on similar topics.

4.1 EUROBAROMETER 46.1: INFORMATION TECHNOLOGY AND DATA PRIVACY

Eurobarometer 46.1: Information technology and data privacy[47] was produced for the European Commission and published in January 1997 by INRA (Europe) who oversaw a series of different polling organisations within the 15 European Union Member States (at that time). The purpose of the survey was twofold; first, the survey aimed to develop a wider understanding of Europeans' interest in information technology; second, the survey sought to show the extent and nature of Europeans' concerns regarding their data privacy. The survey provides individual country results and demographics, allowing for comparisons at levels such as: country, gender, age and education. Although this survey took place following the introduction of the Data Protection Directive 95/46/EC[48] in October 1995, which focused on protecting the rights of individuals with regard to the processing and free movement of their data, there was no discussion of this new legislation within the report.

This survey focuses on the relationship between data privacy and technology and is relevant to our work on PRISMS as it enables us to explore two key themes of our analysis: privacy and trust.

4.1.1 *Methodology*

Between the 19 October and 22 November 1996, a European network of market and public opinion research agencies carried out a series of face-to-face surveys within individuals' homes, using their national language. The survey used a multi-stage cluster sampling strategy to provide a representative sample of targeted individuals who were over the age of 15 in the 15 European Union Member States. The following table (Table 2) provides further details of the sample regarding specific countries and the number of participants questioned.[49]

[47] INRA (Europe), *Eurobarometer 46.1: Information Technology and Data Privacy*, European Commission, January 1997. http://ec.europa.eu/public_opinion/archives/ebs/ebs_109_en.pdf

[48] European Parliament and the Council, Directive 95/94/EC, of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal*, L 281, 23 November 1995. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[49] Any figures included in this report are the property of the authors of this report and have been compiled and referenced accordingly using data from surveys under inspection.

Table 2: Eurobarometer 46.1: Information technology and privacy - sample information[50]

Country	Sample size
Belgium	1006
Denmark	1000
Germany (East)	1008
Germany (West)	1024
Greece	1012
Spain	1000
France	1003
Ireland	1003
Italy	1059
Luxembourg	610
The Netherlands	1070
Portugal	1003
Great Britain	1067
Northern Ireland	324
Austria	1009
Sweden	1008
Finland	1040

In total, 16,246 people across Europe were questioned about their interest in information technology and their concerns around data privacy.

4.1.2 *Main findings*

The survey appears to develop its understanding of the concept of "privacy" via its exploration of participants' perceptions of their information trails, that is, the privacy of individuals' data. At the time of publication, this survey revealed a degree of concern by some Europeans about the consequences of using new information technologies and what this may imply about the safety of their information and, therefore, the privacy of their personal data. The following question was used to understand this:

> The use of some services provided on the networks we have just mentioned, leaves 'electronic tracks', that is pieces of information such as name, address, date of birth, gender. Would you be very worried, quite worried, not very worried or not at all worried about leaving such personal tracks on the networks?[51]

As a whole, results reveal that most of the respondents had some degree of concern over the privacy of their data: not very worried (21%), quite worried (35%) and very worried (32%). Only 12% stated that they were not worried at all.[52]

When considering differences in perceptions across the 15 different countries, the survey revealed that some countries are more concerned over the privacy of their data than others. For instance, in Greece, Portugal and Italy, an equal proportion of people stated that they were "worried" vs. "not worried". However, in the Netherlands and the UK (for instance) the proportion of people who were worried far exceeded those who were not worried (approximately 75% compared to 15%). Thus, in 1996, there appears to have been a degree of

[50] INRA (Europe), 1997, p. 46.
[51] Ibid., p. 16.
[52] Ibid.

divergence across Europe with regard to public concerns over privacy in relation to new information technologies and what their adoption implied for the privacy of data. This may be linked to personal usage of new technologies.

Researchers found differences relating to two demographic variables: gender and age. However, the survey report does not provide an individual country breakdown to enable analysis to extend to see whether this was the same or different across European Member States. In relation to gender, women appeared to be slightly more worried than men. For instance, a slightly higher proportion of men (13%) than women (11%) reported not being worried at all. In contrast, a slightly higher proportion of women (32%) reported being "very worried", in comparison to 29% of men. In relation to age, the older the participant, the more concerned they were; the following figure (Figure 19) outlines how age relates to participants' reported levels of worry:

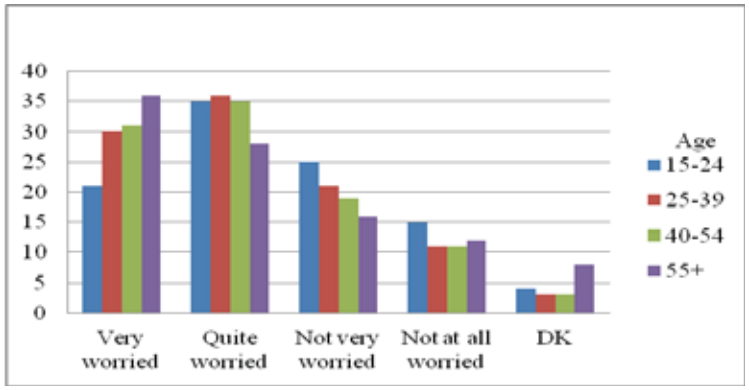


Figure 19: Eurobarometer 46.1: Information technology and privacy - privacy and age[53]

A second measure that the survey used to try to understand Europeans' perceptions of privacy of their data is linked to the use of new technologies from a consumer perspective. Participants were asked about their consumption habits, whether they felt that using new technologies would infringe on the security of their personal data, and whether this would stop them from using new technologies in future transactions. The following question was used:

> Thinking about the ways of paying for goods and services that can be bought on these networks, which of the following opinions comes closest to your own?
> A. I would be prepared to use any means of payments, even those leaving tracks
> B. I would be prepared to use any means of payments, even those leaving tracks, provided this information is used only to enable me to control and check my expenses
> C. I would not be prepared to use means of payments which leave tracks
> D. It depends, I want a choice (spontaneous)
> E. I would not buy any products or services on these networks (spontaneous)
> F. None of these[54]

Results from this question correspond to citizens' privacy concerns as revealed in the previous question. Europeans in 1996 seem to be somewhat undecided in their payment habits; in relation to safeguarding their personal data, 39% answered that they would use the technologies provided that their purpose was to enable consumers to monitor their spending

[53] Ibid., p. 17.
[54] Ibid., p. 22.

(option B) and 32% answered that they would not be prepared to use the technologies at all (option C). Responses seem to be varied across the different European countries questioned. Resistance (option C) seems to be highest in Denmark (45%) and lowest in Greece (20%). Importantly, for those who are willing to use new information technologies, individuals report that they would like some form of control over how their personal information is used (option B – 39%).[55]

In addition to exploring the impact of nationality, age and gender on public opinion of data privacy and new technologies, the survey also produced an analysis of results in relation to educational achievement. Education was categorised according to the number of years spent in full-time education. This may be somewhat limited in terms of understanding the impact of education as it assumes that time spent in part-time education (for instance) is not a contributing factor. In relation to time spent in education and perceptions of data privacy, there appears to be mixed responses. In terms of being "very worried", the longer individuals spent in education, the less worried they were. However, in relation to other levels of worry, the relationship is not so clear. For instance, for those who were "not at all worried", there was very little evidence of the time spent in education affecting this perception, rather, perceptions remained steady across the different levels of education. The following figure (Figure 20) supplies further evidence of this trend:

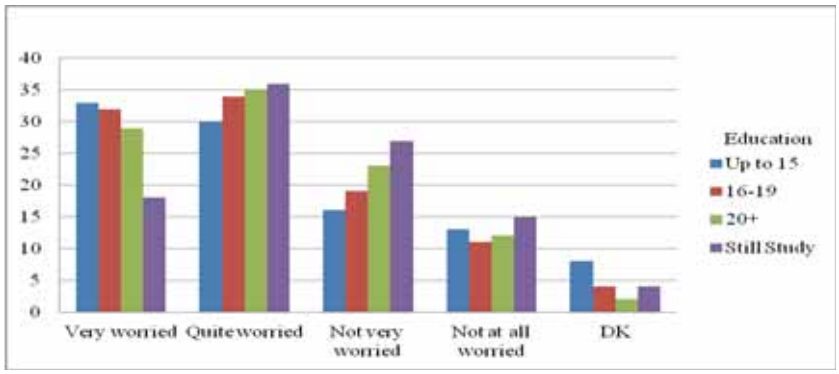


Figure 20: Eurobarometer 46.1: Information technology and privacy - privacy and education[56]

The issue of "trust" is also important for our analysis of surveys in PRISMS. In this survey, the concept of trust appears to be operationalised by asking respondents whether they would want a say in what was done with their data. To an extent, this provides researchers with an indication of whether individuals want control over their data, and therefore, whether they would completely trust their data with others. The following question was used to tap into this area of enquiry:

> Which one or two of the following opinions come closest to your own?
> A. It has to be possible to get access to the services on these networks by giving no or very little personal information
> B. I always want to know who has information about me and what they intend to do with it
> C. I want to be able to give my agreement before information about me is used
> D. It does not matter to me what is done with my personal information, if it enables me to use a new service
> E. If I am told in advance, it does not bother me if companies use information about me to send me advertising leaflets

[55] Ibid., p. 22.
[56] Ibid., p. 18.

F. I want the tracks that I leave on the networks when I use these new technologies to remain confidential or to be erased automatically so that no one can use them
G. None of these[57]

For the most part, respondents indicated that yes, they would want a say in how their personal data was used (approximately 23% and 28% of respondents chose option B and option C respectively). Very few (approximately 3%) responded with "D" in that they were not concerned over who was accessing or using their personal information. In order to understand the link between personal data privacy and desire for personal information to be protected, the survey also asked respondents whether they would want their personal data protected in the European Union as well as across the globe; 63% of respondents indicated that it would be "very important" for their personal information to be protected in the European Union and across the world, while only 2% felt that it was "not at all important". From a demographic perspective, a slightly higher proportion of women (62%) felt that it was "very important" for their data to be protected in the EU and across the world than men (59%). Furthermore, those of a slightly younger age (15-24 years) were not as concerned with the protection of their personal data as those that were older than them; 55% of 15-24 year olds felt it was "very important" for the EU and the rest of the world to protect their personal data as opposed to 62% of those aged 25-39, 63% of those aged 40-54 and 60% of those aged over 55.[58] Unfortunately, results regarding the impact of education on this question were not included in the report.

4.1.3 *Relationship with other surveys*

In relation to other surveys discussed here, *Eurobarometer 46.1: Information technology and privacy* demonstrates that concerns over the privacy of data on the Internet and trust regarding the handling of personal data date back to at least 1997. Elsewhere, results from a study by Vidmar and Flaherty demonstrates that public concern over the invasion of privacy by the government as a result of new technology dates back to at least 1985.[59] As will be seen in other surveys, such as the *Flash Eurobarometer 225: Citizens perceptions of data protection*, these issues have continued, and in some instances (such as in relation to the issue of privacy) have grown in significance. In relation to the nature of questions, questions about trust in the 2008 *Flash Eurobarometer 225: Citizens perception of data privacy* are significantly clearer than those posed here. The Graphic, Visualization and Usability Center's (GUV) 8th WWW User Survey, also from 1997, provides an interesting comparison to this survey, where following an online survey of over more than 10,000 web users, they also recorded an increase in concern over the privacy of data.[60] Thus, concern over privacy in 1997 appears to be not just a European concern, but a global concern.

4.1.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages.

[57] Ibid., p. 24.
[58] Ibid., p. 35.
[59] Vidmar, Neil, and David H. Flaherty, "Concern for Personal Privacy in an Electronic Age", *Journal of Communication*, Vol. 35, No. 2, 1985, pp. 91–103.
[60] GVU Center, *GVU's 8th WWW Survey Results*, GVU's WWW User Surveys, College of Computing, Georgia Institute of Technology, 1997. http://www.cc.gatech.edu/gvu/user_surveys/survey-1997-10/#exec

Eurobarometer 46.1: Information technology and privacy offers our analysis of surveys within PRISMS the opportunity to understand perceptions of privacy and trust with regard to the handling of personal data. The main message received from this survey is that Europeans do indeed feel concerned with the privacy of their data. The survey has revealed that there are noticeable differences in the extent of concern over privacy across different European states. In addition, evidence suggests that Europeans also have concerns over the handling of their data which provides us with an understanding of the extent (or level) of trust attributed to others. As identified in 2.1.3, results from this survey also correspond to other surveys taking place at that time.

4.2 SPECIAL 9/11 POLL – HARRIS INTERACTIVE

The *Special 9/11 Poll* was published by Harris Interactive, a global market research company, in 2002.[61] The present survey was one of four polls that were conducted to develop an understanding of the "mood of Americans"[62] on the anniversary of the terrorist attacks in the USA in September 2001. The aim of the survey was to develop a wider understanding of public support for law enforcement and surveillance measures in the aftermath of the attacks. This survey is particularly useful in that it specifically examines the trade-off between surveillance and security.

4.2.1 *Methodology*

This survey conducted by Harris Interactive was in the form of an online survey in the USA. The survey was placed online between 26 August and 3 September 2002, and Harris Interactive obtained a sample of 2,203 Americans. Where necessary, researchers weighted the figures to bring them in line with the population. The report provided very little information to suggest how respondents were selected; rather a note was included to state the sample was not a probability sample.[63]

4.2.2 *Main findings*

Within the context of this survey, surveillance was investigated with the use of examples of different types of surveillance strategies: a national ID system, expanded camera surveillance on streets and public spaces, law enforcement measures on the Internet and monitoring of communications (cell phone and e-mail). Drawing on these different measures, the poll used the following question to ask whether individuals favoured or opposed them (the option of "don't know" was also given):

> Following are some increased powers of investigation that law enforcement agencies might use when dealing with people of terrorist activity, but which would also affect our civil liberties. For each please indicate whether you would favor or oppose it.

[61] Taylor, Humphrey, *Support for Some Stronger Surveillance and Law Enforcement Measures Continues While Support for Others Declines*, Harris Interactive, 10 September 2002.
http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Support-for-Some-Stronger-Surveillance-and-Law-Enf-2002-09.pdf
[62] Ibid., p. 1.
[63] Ibid., p. 3.

Results reveal that individuals favoured the adoption of a national ID system (60%) and the increase in camera surveillance (58%). However, individuals expressed slightly greater opposition to the monitoring of online forums (45% opposed compared to 42% who favoured this surveillance measure) and cell phone and e-mail communication (55% opposed compared to 32% who favoured this surveillance measure).

The survey also compared these results with previous surveys dating back to three time periods: September 2001, March 2002 and August/September 2002. This comparison provides an indication of how public attitudes have changed over time in relation to the trade-off between security and surveillance. Immediately following the attacks, the level of support for all four measures was substantially higher. With the exception of the national ID system and the camera surveillance, support for the monitoring of the Web and communication has declined. Over time, there has been an overall reduction is support for increasing surveillance:

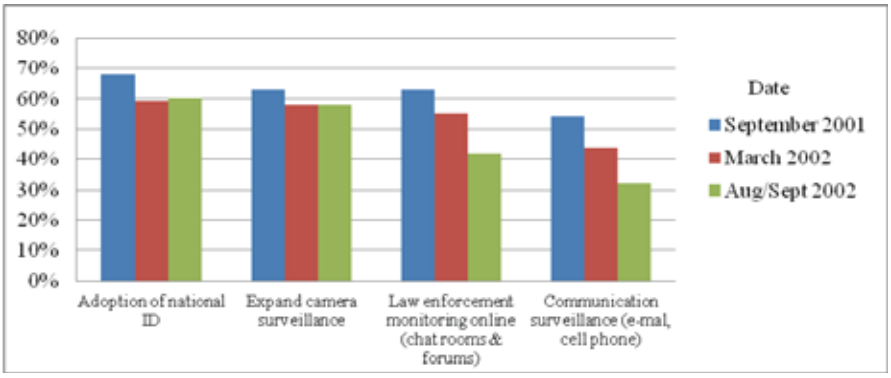


Figure 21: Harris Interactive – Those who favour increased law enforcement and surveillance (2002)[64]

4.2.3 *Relationship with other surveys*

In this survey, some respondents state that it is appropriate to forego their privacy and accept greater surveillance to enhance security. However, a comparison to a Harris Interactive survey from October 2001[65] found that support for surveillance measures that would increase security has declined, with individuals wanting to protect their civil liberties one year later. Further complicating this picture, a telephone survey by Michigan State University[66], published in April 2002, found that some individuals were prepared to trade their civil liberties to enhance their security; approximately 45% were prepared to give up their civil liberties.[67] However, individuals' willingness to sacrifice privacy to enhance their security is limited according to the type of privacy that is exposed. For instance, in relation to the monitoring of telephone and e-mail communications, approximately 34% were willing to trade in their privacy, whilst 67% would prefer to protect their civil liberties.[68] Additional surveys support this finding over time, such as the European *Flash Eurobarometer #225* from 2008, since the public continue to express support for greater surveillance to enhance security, particularly in relation to the fight against terrorism. However, this survey and the *Flash*

[64] Ibid.
[65] Harris Interactive, *Overwhelming Public Support for Increasing Surveillance Powers and, Despite Concerns About Potential Abuse, Confidence That the Powers Will Be Used Properly*, 3 October 2001. http://www.harrisinteractive.com/NEWS/allnewsbydate.asp?NewsID=370
[66] Davis, Darren, and Brian Silver, "Americans Protect Civil Liberties", *Institute for Public Policy and Social Research Policy Brief*, Vol. 4, April 2002. http://ippsr.msu.edu/Documents/PolicyBrief/911Briefing.pdf
[67] Ibid., p. 3.
[68] Ibid., p. 1.

Eurobarometer #225 also reveal that this support is complex, with individuals having a desire to restrict some of these measures. Consequently, whilst there may be acceptance with regard to surveillance measures, there is also a desire to protect civil liberties. This support is, therefore, conditional.

4.2.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages. This survey does not appear to be linked to any publicly available archived press releases or policy deliberations or stories in the press.

This 2002 survey by Harris Interactive is particularly useful for PRISMS as it provides us with an understanding of the trade-off between increasing surveillance measures and security in specific relation to the perceived threat of international terrorism, since the survey was timed to coincide with the anniversary of the 9/11 terror attacks in the USA. Evidence from the survey suggests that whilst American respondents do feel that surveillance is necessary, there is increasing opposition to certain types of surveillance measures such as those that monitor communication from immediately after the event to one year later. This temporal issue is relatively consistent across surveillance technologies or practices, as support for such surveillance measures to provide security was highest immediately after the event, and tailed off as the event retreats further into the past.

4.3 A TWO-EDGED SWORD – PUBLIC ATTITUDES TOWARDS VIDEO SURVEILLANCE IN HELSINKI

A two-edged sword – public attitudes towards video surveillance in Helsinki[69] reports the findings of a survey concerning surveillance that was conducted in Helsinki, Finland in 2003. The survey was conducted by The City of Helsinki Urban Facts, a research institute in Helsinki. The study aimed to understand public attitudes towards increasing numbers of surveillance technologies and how these surveillance technologies are able to influence public perceptions of security.[70] This survey is relevant to PRISMS as it provides an insight into attitudes towards increasing surveillance in relation to security in Finland, a country that was not represented in the *URBANEYE: CCTV in Europe* project on surveillance in Europe, described in section 2.4 below.

4.3.1 *Methodology*

The research involved a postal questionnaire that was addressed to a random sample of 2,000 individuals in Helsinki between the age of 16 and 69. Addresses were provided to the researchers by the Finnish population register centre. Overall, the sample consisted of 1,240 respondents gaining a response rate of 62%,[71] although the researchers do not indicate whether this is a representative sample. Unfortunately, the report also does not contain any indication of the questions used in the survey and is therefore somewhat limited.

[69] Koskela, 2003.
[70] Ibid., p. 1.
[71] Ibid., p. 2.

4.3.2 *Main findings*

When considering the impact of surveillance technologies on security, results from the survey revealed that 70% of respondents believed the surveillance cameras were "useful" for investigating crime, and 58% believe that the cameras were useful for their abilities to prevent crime.[72] For those in Helsinki, the report indicated a positive attitude towards the usefulness of surveillance cameras in assisting and enhancing security.

When considering how respondents felt about being targeted by surveillance cameras, the report indicated a positive attitude towards cameras. Of the entire sample, 63% stated that it was a good thing for public spaces to be watched over, one third of respondents stated that the presence of surveillance technologies enhanced their sense of personal safety. Respondents were also likely to accept the presence of surveillance technologies as being part of everyday life; as stated in the survey report, only a minority held a negative attitude (although no indication was given in the report as to the size of this "minority").[73]

Researchers also asked respondents where they thought it was suitable for surveillance cameras to be placed. Respondents were more likely to hold a positive view of the use of surveillance cameras in public spaces (90%). However, a majority were less likely to support the use of surveillance cameras in private spaces such as fitting rooms or public toilets.[74]

The survey revealed also sought to explore public attitudes towards who should be trusted with accessing and using surveillance technologies. On the whole, individuals seem to be more in favour of "police, watchmen and business owners"[75] being able access video surveillance. However, respondents were less happy for individuals to freely use surveillance cameras; only 2% stated that they were happy for "private persons" to use "surveillance cameras freely".[76] Respondents seem to be in favour of user permits for individuals to have access to video surveillance, something that was not available in Finland at the time.[77]

4.3.3 *Relationship with other surveys*

Other surveys, including the *URBANEYE: CCTV in Europe* project (2004), identified a correlation between where surveillance cameras are placed and whether an individual supports its use. In addition, as revealed in other surveys included in this analysis, such as *URBANEYE: CCTV in Europe* (2004) and The Globalization of Personal Data (2008), video and camera surveillance appears to be a technology that is largely accepted and supported in relation to enhancing security.

4.3.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages. A link to this survey has

[72] Ibid., p. 3.
[73] Ibid.
[74] Ibid.
[75] Ibid., p. 4. Note: The survey report does not explain the term "watchmen". Similarly, the report provides no statistics to describe the size of the "majority".
[76] Ibid.
[77] Ibid.

been provided by the European Urban Knowledge Network, a knowledge hub providing a network for policy-makers, practitioners and researchers interested in matters relating to urban development.[78]

Although somewhat limited in sample size and location, this survey has revealed that individuals hold a positive view of the use of one particular surveillance technology, CCTV systems, to enhance security, provided it is placed in spaces where individuals have little expectation of privacy. As other research and surveys have indicated, individuals are less supportive of the use of surveillance technologies, and CCTV in particular, in spaces such as changing rooms and toilets where there is an expectation of privacy. This wide support sits in contrast to waning support for the use of communication surveillance technologies described in the *Special 9/11 poll* discussed above and the use of biometric technologies in the *Financial Times/Harris Poll: Body scanners*, described in section 2.14 below.

4.4 URBANEYE: CCTV IN EUROPE

URBANEYE: CCTV in Europe[79] was published in August 2004, and was the result of a comparative project funded by the European Commission under the Fifth Framework Programme (FP5)[80]. The project consisted of a range of research activities to develop a wider understanding of the presence of CCTV as a particular surveillance technology in both public and private spaces in Europe. The project also aimed to assess the implication of the expansion of CCTV within Europe and to make policy recommendations to help support decision-makers in developing future policies. Whilst this project involved a series of research elements, of particular relevance to PRISMS is *URBANEYE: CCTV in Europe*'s consideration of the social effects of CCTV and the project's examination of public attitudes regarding CCTV in Europe. Thus, this portion of the *URBANEYE: CCTV in Europe* research has relevance for PRISMS in relation to all four categories: surveillance, privacy, security and trust.

4.4.1 *Methodology*

The investigation into the social effects of CCTV within the *URBANEYE: CCTV in Europe* project involved a quantitative, street survey that took place between 1 June and 24 October 2004. The survey's sample consisted of 1,001 participants from five European cities: Berlin, Budapest, London, Oslo and Vienna. The survey was followed up with 30 in-depth interviews with respondents that had originally participated in the quantitative survey: "school children, marginalised people such as drug users and informants from their wider social networks".[81] Researchers aimed to secure participants within urban public spaces, preferably close to shopping malls, however, this was not always possible. Despite this form of availability sampling, *URBANEYE: CCTV in Europe* researchers considered their sample to contain a

[78] European Urban Knowledge Network, "EUKN - 'A Two-edged Sword' - a Research on the Attitudes of Helsinki Citizens Toward Video Surveillance", 16 October 2003. http://www.eukn.org/E_library/Security_Crime_Prevention/Crime_Prevention/Camera_Surveillance/A_two_edged_sword_a_research_on_the_attitudes_of_Helsinki_citizens_toward_video_surveillance

[79] Hempel and Topfer, 2004.

[80] "Welcome to the URBANEYE Project on CCTV in Europe", URBANEYE, 2004. http://www.URBANEYE.net/index.html

[81] Hempel and Topfer, 2004, p. 42.

sufficient balance with regard to gender and education, although those aged between 15 and 39 were overrepresented.[82]

4.4.2 *Main findings*

Social attitudes measured in this survey relating to the presences of CCTV in public and private spaces suggest that individuals are predominantly supportive of the use of CCTV in all five countries. Support was found to be in higher in Britain (94.4%) than in Austria (45.5%) and Germany (56%).[83] When considering support by age, the most supportive group were those over the age of 60 (76.7%), those aged between 20 and 39 were more critical (29.7%).[84]

Respondents were also asked to rate their attitudes in terms of the location of cameras. Options from which individuals could choose included: good, bad or neutral. Results from the survey suggested that opinions differed based on the location of the camera. For instance, in relation to whether a location was "good", cameras in public spaces, such as bank counters (91.9%) and train platforms (86.7%) yielded greater support than in private spaces such as a public toilet (22.2%) or a clothing store changing room (13%) – perhaps a sign of the extent of privacy an individual may feel is being exposed.[85]

To further understand participants' attitudes towards CCTV, researchers presented respondents with a series of positive and negative statements about CCTV and asked if they agreed or not. Respondents reported the greatest amount of optimism in relation to the view that CCTV yielded the power to displace crime; 50.5% of respondents agreed with this statement. Optimism seemed to be greater in relation to the statement "nothing to hide, nothing to fear"; 66.4% of respondents agreed with this statement. Fewer than 50% of individuals felt that CCTV was a violation of their privacy (41.4%). A further 44.3% agreed with the statement that hidden cameras were okay. [86]

When introducing demographic categories into understanding public attitudes, the researchers found little difference between positive and negative views of CCTV cameras by gender.[87] Alternatively, researchers found that age was an important factor to public attitudes; older people were identified as being more likely to hold a positive view of CCTV than younger people.[88]

However, the cities in which respondents lived did have a correlation with their views on CCTV cameras. The survey found that those in London, for instance, seemed to hold a much more positive view of CCTV cameras: 67.2% felt that hidden cameras were okay (compared to only 6% in Vienna). In addition, Londoners seemed to be more in favour of welcoming the use of CCTV on their street (68.5% agreed with this statement compared to only 3.5% in Vienna). The survey was also able to establish a relationship between CCTV and security; those in London were much more inclined to feel that CCTV would make them feel

[82] Ibid., p. 40.
[83] Ibid., p. 44.
[84] Ibid.
[85] Ibid., p. 43.
[86] Ibid., p. 46.
[87] Ibid. Note: Statistics were not provided within the report to indicate different responses to this question by gender and age. Rather, conclusions presented here stem from those presented by the researchers.
[88] Ibid.

physically safer (45.6% agreed with the statement); in contrast, only 3.5% of those in Vienna held this view.[89]

Finally, *URBANEYE: CCTV in Europe* considered public views on regulation of operating and using CCTV systems. The researchers found that "the majority of respondents prefer the police to operate an open street CCTV system" than other organisations. Across all cities surveyed, respondents felt that it was "very important" for the media to have restricted access to CCTV systems (80.9%). They also indicated that CCTV systems should be restricted to those that had commercial interests (79.5%). Participants were less inclined to state that the police should have restricted access (29.9%).[90] Thus, findings from the *URBANEYE: CCTV in Europe* study suggest that citizens are more trusting of the police in operating CCTV systems than private bodies.

4.4.3 *Relationship with other surveys*

Results from this survey yield similar results found in two other surveys included in this analysis. The *Special 9/11 Poll* by Harris Interactive (2002), presented above, found similar levels of support for the use of surveillance technologies. Furthermore, the results of the *Personlig Integritet: Perceptions of privacy in public spaces* (2008), found that Swedish individuals were more suspicious of CCTV being a violation of their privacy than Americans. Here, as in *Personlig Integritet: Perceptions of privacy in public spaces*, Europeans report being relatively mistrustful of CCTV as a potential violation of privacy.

These survey results are somewhat refuted by results from a 2007 Gill et al. study on the use of CCTV in residential areas in the UK.[91] Their study consisted of two stages of surveys. The first survey was conducted in six residential estates prior to the implementation of CCTV between January 2002 and January 2003. The second survey returned to these estates approximately 12 months later following the implementation of CCTV systems.[92] In the first instance, support for CCTV declined between pre- and post-implementation of the CCTV systems.[93] The survey also found that prior to installation of CCTV systems, public attitudes indicated that "slightly more than 16% of respondents perceived CCTV as an invasion of privacy".[94] However, following installation of CCTV systems, there was a "reduction in the proportion of respondents concerned with civil liberties".[95] Thus, in this instance, concern over privacy decreased following installation of CCTV systems, although support for CCTV also decreased at the same time.

4.4.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages.

---

[89] Ibid.
[90] Ibid., p. 47.
[91] Gill, Martin, Jane Bryan and Jenna Allen, "Public Perceptions of CCTV in Residential Areas", *International Criminal Justice Review*, Vol. 17, No. 4, 1 December 2007, pp. 304-324 [p. 321].
[92] Ibid., p. 307.
[93] Ibid., p. 319.
[94] Ibid., p. 321.
[95] Ibid.

The *URBANEYE: CCTV in Europe project* on CCTV in Europe revealed that, as of 2004, many Europeans appeared to support CCTV surveillance in their lives. However, results from the survey also suggest a level of suspicion and concern in relation to CCTV, particularly with regard to the misuse of information and the violation of privacy. These results vary across different European countries, with those in London being more supportive and less concerned than those in Vienna and Berlin. Results from this survey also suggest that individuals do care about where CCTV cameras are located, with respondents being more supportive of CCTV in public spaces rather than private spaces.

4.5 E-IDENTITY: EUROPEAN ATTITUDES TOWARDS BIOMETRICS

e-Identity: European attitudes towards biometrics[96] is a white paper that was published in 2006 by Logica CMG, a London-based IT service company. The purpose of the *e-Identity: attitudes towards biometrics* survey was to explore public opinion towards the introduction of biometric technology in Europe, particularly with regard to future products relating to identity and financial security. This survey enables us to further understand European attitudes towards a particular surveillance and security technology – biometrics.

4.5.1 *Methodology*

Research for the 2006 *e-Identity: attitudes towards biometrics* survey was conducted for Logica CMG by an independent research company, Vanson Bourne. The survey was conducted in April 2006 and gained a sample of 500 respondents from seven European countries: the UK, France, Germany, the Netherlands, Spain, the Czech Republic and Portugal.[97] Little information regarding the survey's methodology was included in the white paper. Accordingly, we cannot analyse the nature in which the survey was administered or specific sample information. In particular, it is unclear whether the sample was representative.

4.5.2 *Main findings*

Throughout the survey, respondents were asked a series of questions designed to elicit whether they felt biometrics, such as fingerprint and iris scanners, were viable options for identity management in relation to financial transactions and whether they could replace more established proof of identity measures, such as a signature. The survey seemed to demonstrate a great deal of support and favour (more than 50%) of biometrics as a more secure measure across Europe. However, this support was higher in some countries, such as Portugal and France, and lower in Germany and the Netherlands. An example of a question that sought to probe perceptions in this area included whether respondents think biometrics could reduce financial fraud during a transaction. The following question was asked:

> Do you think financial fraud could be reduced if you had to use your thumb print in association with an ID card to make a financial transaction?[98]

In all countries, there was a positive response to this question. Most individuals (more than 50%) in all countries produced a positive response to this question; the country with the

[96] Logica CMG, *e-Identity: European Attitudes Towards Biometrics*, 2006. http://www.eurokiosks.org/whtpapers_logica_e_identity.html
[97] Ibid., p. 3.
[98] Ibid., p.4.

greatest degree of agreement was Portugal (90%), while the lowest degree of support was seen in Germany (approximately 70%).[99]

An additional question that sought to understand how individuals felt about the security of biometric technology asked respondents whether they thought fingerprints were more secure than a signature for identity checks. As with the previous question, in all countries, more than 80% of respondents felt that fingerprints were more secure. Again, agreement was highest in Portugal and France (approximately 90%) and lowest in Germany and the Netherlands (approximately 80%).[100]

A final example of support is linked to identity checks while travelling abroad. Respondents were asked:

> Would you be happy using your fingerprint or having a scan of your eye taken in order to prove who you are when travelling abroad?[101]

Responses to this survey reveal that there seems to be more support than opposition to the use of biometrics in identity management when travelling. In contrast to other questions, there does, however, seem to be greater opposition to this question in the Czech Republic; approximately 30% of participants stated they would not be happy; in contrast, approximately 67% stated they would be happy.[102] Whilst individuals may think that e-identity technologies are more secure, this does not necessarily mean that individuals would automatically be willing to personally adopt these measures.

4.5.3 *Relationship with other surveys*

Other surveys included in this analysis, such as the *State of the Nation* (2010), suggest that individuals are willing to support the introduction of surveillance technologies to enhance their security. Like findings related to CCTV, some surveillance technologies enjoy strong support in Europe. However, as revealed by *The Globalization of Personal Data* project in 2008, some individuals do not seem to know much about what biometrics involve. However, results from the next survey, *A Survey on EU Citizens' Trust in ID Systems and Authorities*, challenge these findings and indicate that individuals do not necessarily trust e-identity technologies.

4.5.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages. The survey has been cited by other European Commission funded projects such as FIDIS.[103]

This survey by Logica GCM explores public opinion towards the introduction of biometric technologies in Europe. Results suggest that there is support for the implementation of

[99] Ibid.
[100] Ibid., p. 5.
[101] Ibid., p. 6.
[102] Ibid.
[103] Backhouse, James, and Ruth Halperin, *D4.5: A Survey on Citizen's Trust in ID Systems and Authorities: Future of IDentity in the Information Society*, FIDIS Project Deliverable 4.5, 17 April 2007. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.5.a_survey_on_EU_citizens_trust.pdf

biometric technologies to enhance individuals' security and identity management. However, because of a lack of information, it is not possible to conduct a demographic analysis beyond individual countries samples or to adequately examine the sample design.

4.6 A SURVEY ON EU CITIZENS' TRUST IN ID SYSTEMS AND AUTHORITIES

In 2006, James Backhouse and Ruth Halperin at the London School of Economics and Political Science conducted and published *A survey on EU Citizens' Trust in ID Systems and Authorities*.[104] The survey was undertaken as part of the work on the FP6-funded project FIDIS "The Future of Identity in the Information Society".[105] This survey aims to develop an understanding of Europeans' attitudes towards the implementation of ID systems and trust in authorities that manage and implement these systems. Accordingly, this survey is important to PRISMS as it focuses on the themes of privacy and trust.

4.6.1 *Methodology*

The survey was an online survey translated into eight European languages, and took place in June 2006 over a period of one month. In addition to being asked 10 demographic questions, the survey employed a seven point Likert scale (1 – strongly agree, 7 – strongly disagree) for 32 different statements. The survey was promoted to personal contacts of the research team, press releases and advertisement on project websites as well as project partners' websites. In total a sample of 2,918 responses were gathered from 23 out of 25 European countries. However, as some of the respondents were not from an EU Member State, this was reduced to 1,907 responses.[106] Unfortunately, as outlined in the report, the sample obtained was not representative of Europeans, thus findings must be considered with caution. Researchers analysed responses in terms of five regional clusters rather than by country: 1) UK and Ireland; 2) Austria, Germany and Scandinavia; 3) the Benelux countries and France; 4) Central and Eastern Europe and 5) Southern Europe.[107] In addition to problems relating to the nationality of respondents, the sample was also heavily weighted towards male participants (1,579 vs. 327 females).[108] The mean age of respondents was 33.85 years, thus the survey is also limited in representation of different age groups.[109]

4.6.2 *Main findings*

This survey sought to emphasise the degree of trust Europeans have in the implementation of electronic ID systems by organisations. Overall, when considering the compilation of results across Europe, respondents reported a rather negative view with regard to trusting others with personal data.[110]

When considering the implementation of ID systems, respondents reported negative attitudes towards both the degree of control they would have over their own data and the availability of

[104] Backhouse, James, and Ruth Halperin, "A Survey on EU Citizens' Trust in ID Systems and Authorities", *FIDIS Journal*, No. 1, June 2007.
http://journal.fidis.net/fileadmin/journal/issues/1-2007/Survey_on_Citizen_s_Trust.pdf
[105] FIDIS project, "Future of IDentity in the Information Society", n.d. http://www.fidis.net/
[106] Backhouse and Halperin, *A Survey on EU Citizens' Trust in ID Systems and Authorities*, 2007, p. 13.
[107] Ibid., pp. 14-15.
[108] Ibid., p. 17.
[109] Ibid., p. 16.
[110] Ibid., p. 25.

appropriate policies to regulate external use of public data. Mean scores in both these categories were no more than 5 on the Likert scale. The study also found differences in perceptions in different regions. With regard to control over data, those in the UK and Ireland were more likely to hold a positive view (6.1 on the Likert scale) than those in Central and Eastern Europe (3.9 on the Likert scale). In relation to views over appropriate policies, respondents in Southern and Central/Eastern Europe held negative views (3.8 and 3.1 respectively). Respondents were also inclined to believe that the ID data systems would be technically insecure and thus did not have much trust in the security behind the storage of their data.[111]

The second area of enquiry relevant to PRISMS is the degree of trust individuals have in those responsible for managing ID systems (referred to as ID authorities). Across Europe, findings suggest a lack of trust in the competence of authorities being able to manage ID data. Scores were higher in the UK and Ireland (6.0 on the Likert scale) and lowest in Central and Eastern Europe (4 on the Likert scale).[112]

Researchers also measured trust in ID authorities in terms of whether respondents felt ID authorities would be of assistance if something went wrong. Once again, this line of enquiry received a negative response across Europe.[113] In relation to age, the older the respondent, the more they were likely to believe that ID authorities would not be trustworthy when something went wrong. For instance, 21% of those aged between 15 and 24 gave a score of 7, whilst 38% of those aged 40 and above were more likely to respond with a score of 7.[114] The level of distrust towards authorities is exemplified in the belief that authorities will use and access personal data without permission.[115]

Whilst this survey provides useful information in relation to trust, it also offers some explanation of how respondents would deal with sharing their own personal data. The survey found that respondents were only partially willing to reveal their personal data (mean score of 4.8).[116] Despite the high levels of concern, there seemed to be reluctance on the part of individuals to have their data removed from unauthorised lists; however, the report did not provide any reason for this.[117]

4.6.3 *Relationship with other surveys*

In some ways, findings from this 2006 survey clash with those identified by the Logica CGM 2006 survey on attitudes towards the implementation of e-identity technologies. Findings from this survey conducted by LSE suggest that individuals have little confidence in e-identification, yet findings from the 2006 Logica survey suggest an optimistic attitude towards the implementation of e-identification systems, with individuals believing that e-technologies are more secure. However, the authors of the Logica survey report also found that some individuals were less happy about the *personal* use of e-identity technologies. Differences in results may be linked to the nature of questioning and inadequate samples contained within the project; specifically, this survey involved self-selected respondents

[111] Ibid., p. 18.
[112] Ibid., p 21.
[113] Ibid. Note: Individual scores were not given for different regions.
[114] Ibid.
[115] Ibid., p. 22.
[116] Ibid., p. 23.
[117] Ibid., p. 24.

beginning with those already interested in issues related to privacy, security and trust, through the use of the designers' personal contacts and the project's contacts and website visitors.

4.6.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages. The survey has been cited by other European Commission funded projects such as FIDIS.[118]

Results from this survey suggest a lack of confidence in officials' handling of e-identification technologies. Furthermore, public opinion also suggests a distrustful perspective of the security behind these technologies. Whilst these results seem to differ from previous surveys, this may be partially related to the fact that the sample involved self-selection and was not representative of the European population.

4.7 PEW INTERNET & AMERICAN LIFE PROJECT: DIGITAL FOOTPRINTS

The *PEW Internet & American Life Project: Digital Footprints* study[119] focuses on understanding how individuals are managing the increasing amount of information that they are revealing about themselves online, in other words, their personal "digital footprint". The survey was conducted in 2006 and the results were published and made publicly available for viewing in December 2007. The survey offers the PRISMS project the opportunity to consider the growing impact of sharing personal information online and what this implies for the privacy of personal data. Of particular relevance to the PRISMS analysis, this survey examines the various measures respondents were taking to limit other people's access to their personal data.

4.7.1 *Methodology*

The Digital Footprints study consisted of a survey of American nationals which took place from 30 November to 30 December 2006. The survey was carried out by Princeton Survey Research Associates International, and was in the form of a telephone survey. The final sample consisted of 2,373 individuals over the age of 18, and was collected using a random digit sample of telephone numbers that had been taken from telephone exchanges in the US.[120]

4.7.2 *Main findings*

In relation to privacy, the survey begins by asking respondents how concerned they were with their privacy (on the Internet) at that point in time. However, the following question demonstrates that they survey did not give respondents much indication of how they defined the term "privacy":

> Some people are concerned about their privacy today. We'd like to know how you feel about this topic. As I read the following, please tell me how important, if at all, each one is to YOU

[118] Backhouse and Halperin, *D4.5: A Survey on Citizen's Trust in ID Systems and Authorities*, 2007.
[119] Madden et al., 2007.
[120] Ibid., p. 40.

> personally. Is this very important to you, somewhat important, not too important, or not important at all?[121]

The survey then asked respondents to examine this question in relation to three scenarios:

a) Controlling who has access to your personal information
b) Not being monitored at work
c) Having individuals in social and work setting not ask you things that are highly personal[122]

Respondents indicated that it was very important to them to control who had access to their information (85%); only 3% indicated that this was not important at all. In relation to being monitored at work, concern was not as strong: 28% felt that it was very important, 26% answered that it was somewhat important, while others indicated that it was not too important (14%) and not important at all (15%). The final scenario, regarding not being asked private information in a social and work setting, triggered a strong response in that participants were more likely to answer that they felt it was very important to them (42%), as opposed to it not being important at all (10%).[123]

The survey supplemented this initial question with a different approach to investigating public perceptions of privacy; it focused on understanding the digital footprint, i.e., the personal information left behind individuals on the Web, and how people felt this impacted their privacy. The following question sought to understand how users felt about their digital footprint:

> Do you ever worry about how much information is available about YOU online, or is that not something you really worry about?[124]

Results from this question suggest that the majority of respondents (60%) do not worry about the amount of personal information available online.[125] From a demographic perspective, findings from the survey suggest that those younger and older participants indicated a "laissez-faire" attitude towards their personal information.[126] For personal information to be made available online, the individual plays a role in the posting of this content. Accordingly, researchers used the following question to understand if an individual was aware of how much information about them was available on the Internet:

> We'd like to know if any of the following information about YOU is available on the internet for others to see – it doesn't matter if you posted it yourself or someone else posted it. As I read each item, you can just tell me yes or no – if you're not sure if something is on the internet, just say so and I'll move on.[127]

Researchers identified the following results:

---

[121] Princeton Survey Research Associates International, *PEW Internet & American Life Project, December 2006 Tracking Survey: Final Topline*, 1 May 2007, p. 2. http://www.pewinternet.org/Reports/2007/Digital-Footprints.aspx
[122] Ibid., p. 2.
[123] Ibid.
[124] Ibid., p. 26.
[125] Ibid.
[126] Madden, et al., 2007, p. 30.
[127] Princeton Survey Research Associates International, 2007, p. 20.

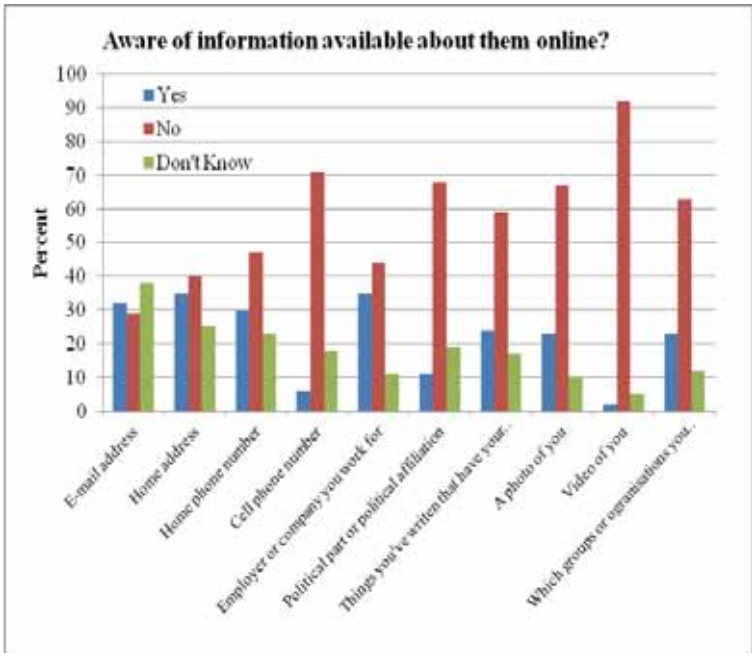


Figure 22: PEW Internet & American Life Project: Digital footprints – participants' awareness of information available about themselves online[128]

Figure 22 (above) indicates that with the exception of a person's e-mail address participants were more likely to report that they were not aware of any of these types of information about them being available online. Types of information that were more readily available include: personal e-mail address, home address and the name of the company or employer for whom people work. Participants were more likely to indicate that personal information in the form of video footage and their cell phone numbers was not available. In all categories, there were some individuals who indicated that they were not sure whether information was available, particularly in relation to their e-mail address.

With such an abundance of personal information available online, the survey proceeded to question participants about the various measures they might be choosing to limit the amount of information available about them. Results reported that the majority of adults (61%) had not taken any measures to limit the amount of information that was available about them on the Internet, although a significant minority (38%) indicated that they had. For those who had taken measures to restrict sharing their personal information, they were more likely to be knowledgeable of the amount of information that was available about them. For instance, one question asked whether individuals had taken the time to search for information about themselves; 46% of those who had searched for their personal information also responded that they had taken measures to restrict access to their information. Only 32% of individuals that had not searched for their personal information online had taken measures to restrict access to their personal information.[129]

This sharing of personal information may be (in part) linked to whether people have a profile on a social networking website. The survey included the following question and gave an example of a social networking website for clarification:

[128] Ibid.
[129] Madden, et al., 2007, p.30.

> Have you ever created your own profile online that others can see, like on a social networking site like MySpace or Facebook?[130]

Results from this survey suggest that the majority (55%) of participants with a profile on a social networking website from this sample were teens; only 20% were adults. Of those who had a profile on a social networking site, adults were somewhat more likely than teens to ensure that their profile is visible for others to see (82% vs. 77%).[131] With regard to adults' use of privacy settings in relation to the visibility of their profile, 60% reported that their profile settings ensure that anybody could see anything included on their profile, whilst 38% indicated that they made use of privacy settings and restricted the visibility of their profile to friends only.[132] Similarly, when comparing this to teens, teenagers appeared to also maintain control over the visibility of their profile: 59% answered that only their friends could see their profiles, while 40% allowed anyone to see their profile.[133]

Since researchers involved in this survey saw some difference in measures taken to enhance privacy on the Internet, they devised four categories of Internet users:[134]

1. *Unfazed and Inactive:* The largest group (43%), they do not worry about their privacy, nor do they take any measures to limit the availability of their personal information.
2. *Concerned and Careful:* The second largest group (21%), they worry about their privacy and take measures to limit the availability of their personal information.
3. *Worried by the Wayside:* This group consists of 18% of users; they are worried about their privacy online, but do not take any measures to limit the availability of their personal data.
4. *Confident Creatives:* The final and smallest group consists of 17% of users; they worry about their privacy, and they do take the time to actively create content on the web; however, they also take measures to limit the availability of their personal data.

4.7.3 *Relationship with other surveys*

As with many of the surveys included in this analysis, such as the *Flash Eurobarometer 225: Citizens perceptions of data protection* (2008) and *Privacy 2.0* (2009), this survey has revealed that individuals are concerned about sharing their personal information online. Additionally, these findings are somewhat similar to those identified by a survey on social network users by Lawyers.com from 2010, who found that some individuals are concerned about how their personal information can be used against them.[135] The PEW survey has also revealed similar findings to the *Flash Eurobarometer 225: Citizens perceptions of data protection* (2008) in that some people are taking measures to enhance privacy, but many are not. In part, these findings support those from a survey conducted by Harris Interactive in 2003. That survey identified a group of what Harris Interactive referred to as "privacy pragmatists". These "privacy pragmatists" consisted of individuals who were concerned about their privacy, but were not necessarily taking appropriate measures to protect themselves.[136]

---

[130] Ibid., p. 25.
[131] Ibid., p. 20.
[132] Ibid.
[133] Ibid.
[134] Ibid., p. 31.
[135] "Lawyers.com 2010 Social Networking Survey Press Release", *Lawyers.com*, 2010. http://press-room.lawyers.com/Lawyerscom-2010-Social-Networking-Survey-Press-Release.html
[136] Harris Interactive, "Most People Are 'Privacy Pragmatists' Who, While Concerned About Privacy, Will Sometimes Trade It Off for Other Benefits, Says Harris Interactive Survey", *The Free Library*, 19 March 2003. http://www.thefreelibrary.com/_/print/PrintArticle.aspx?id=98931112

4.7.4 *Use of the survey results*

This survey attracted interest from a range of different groups. Technological news websites highlighted the survey, and *Technewsworld* featured an article that summarised and critically reviewed its findings. For instance, the author, Katherine Noyes, refers to comments by the director of the Electronic Privacy Information Center (EPIC), who stated that policy-makers and companies should help provide the tools to assist individuals in maintaining their privacy.[137] Other news-based websites also shared results of the study with those who may be vulnerable and may not entirely comprehend the consequences of not placing greater importance on limiting the sharing of personal data. For instance Aly Adair, writing for the *Yahoo! Voice,* discusses this survey by PEW, as well as additional surveys by CareerBuilder, to encourage readers to consider how their actions could impact their options for gaining a job or being accepted to college.[138]

Bloggers also used their personal blogs to repeat news of the findings of the study. For instance, Betsy McKenzie provides a link to the official report by PEW in a blog titled *Out of the Jungle,* which focuses on legal information, research and education.[139] The post focuses on repeating the information rather than analysing it; however, McKenzie encourages others to consider their own activities on the web by considering what writing a blog means for her own privacy. Elsewhere, a blog run by Amber Case, titled "Cyborg Anthropology" used the survey to help define the term digital footprint, although the blog post does not provide any commentary or discussion of the results of the study.[140] A third way in which bloggers used the survey is exemplified by a post written by Ben Turner.[141] Turner's post states that he wanted to find out more about "online culture" within the US. He then goes on to introduce the study by PEW which was relevant to his area of interest. Throughout the post, Turner discusses the results that he finds particularly interesting. He also provides commentary on what he believes the focus will be in the future for US citizens. He states that rather than being concerned about privacy, users will "demand that we have control of our content".[142]

This survey stands out in its exploration of behaviour influencing attitudes towards privacy online. The survey demonstrates that of the majority of individuals who are choosing to share private information about themselves online, some are worried about the availability of this information, but very few actually take measures to enhance their privacy. From the perspective of PRISMS, this survey's approach to understanding privacy on the Internet in contemporary society is fresh and somewhat different from other surveys included in this analysis. Its emphasis on personal involvement in the sharing of information provides a way of understanding how important privacy concerns are, particularly if people are not necessarily taking the time to enhance their privacy. However, the survey does not examine respondents' level of knowledge about how to change privacy settings, in contrast to the

---

[137] Noyes, Katherine, "Pew Study: Self-Googling on the Rise", *Technewsworld*, 17 December 2007. http://www.technewsworld.com/story/Pew-Study-Self-Googling-on-the-Rise-60810.html

[138] Adair, Aly, "Will Your Digital Footprint Cost You a Job and College Admission?", *Yahoo! Voices*, 24 February 2009. http://voices.yahoo.com/will-digital-footprint-cost-job-college-2741408.html?cat=3

[139] McKenzie, Betsy, "Out of the Jungle: Digital Footprints Report from Pew", Blog, *Out of the Jungle*, 17 December 2007. http://outofthejungle.blogspot.co.uk/2007/12/digital-footprints-report-from-pew.html

[140] Case, Amy, "Digital Footprint", Blog, *Cyborg Anthropology*, 23 October 2010. http://cyborganthropology.com/Digital_Footprint

[141] Turner, Ben, "Americans' Attitudes on Digital Footprints (Pew Internet & American Life Project)", Blog, *Ben Turner's Blog*, 10 September 2009. http://blog.benturner.com/2008/09/10/americans-attitudes-on-digital-footprints-pew-internet-american-life-project/#more-1310

[142] Ibid.

Flash Eurobarometer 225: Citizens perceptions of data protection which is discussed in the next section.

4.8 FLASH EUROBAROMETER 225: DATA PROTECTION IN THE EUROPEAN UNION - CITIZENS PERCEPTIONS

Flash Eurobarometer 225: Data Protection in the European Union – Citizen perceptions was published in 2008 and focuses on understanding citizens' views of data protection within the European Union.[143] The survey, assigned by the European Commission, was co-ordinated by The Gallup Organization, a research organisation that specialises in (among other areas of consultancy) public opinion polls. The survey focuses its attention on areas relating to data protection in the European Union; examples include: awareness of data privacy rights, awareness of national data protection authorities and awareness of data protection on the Internet.

This Flash Eurobarometer is particularly relevant to PRISMS as it focuses on exploring all four of our areas of interest: public perceptions of data privacy, the issue of trust in relation to organisations handling of privacy data, perceptions of data security on the Internet and surveillance on the web. Importantly, this survey also offers the opportunity to examine what measures European citizens may be taking to enhance their security on the Internet.

4.8.1 *Methodology*

The survey was conducted in January 2008; the results were subsequently published in February 2008. The survey used two forms of data collection: telephone surveys and face-to-face surveys (where telephone connections were less widespread). The survey consisted of a representative sample of 1,000 individuals over the age of 15 from the 27 European Union Member States.[144] The final report does not include any information regarding the sampling strategy used to select participants; however, it does discuss weighting strategies employed to ensure that the sample was representative.[145]

4.8.2 *Main findings*

Results from this survey suggest that the majority of Europeans do have some concerns, and therefore lack trust, in relation to the handling of their personal data by organisations. Gallup used the following question to understand this area of concern in relation to data privacy:

> Different private and public organisations keep personal information about people. Are you concerned or not that your personal information is being protected by these organisations?[146]

Within this question, the survey designers operationalised privacy by providing participants with an illustrative question where they are told that their personal data is held by both private and public organisations. The survey then asks respondents to answer whether they are

[143] The Gallup Organization, *Data Protection in the European Union: Citizens' Perceptions - Analytical Report*, Flash Eurobarometer Series #225, March 2008.
http://ec.europa.eu/public_opinion/archives/flash_arch_239_225_en.htm
[144] Ibid., p. 128.
[145] Ibid., p. 129.
[146] Ibid., p. 7.

concerned about the protection of their data by organisations. Overall results suggest that at the time of the survey Europeans were concerned with the handling of their personal data by organisations: 30% stated they were "fairly concerned", 34% indicated they were "very concerned".[147] When comparing results between different European countries, one finds significant differences in the nature of responses. For instance, those individuals in Austria and Germany seem to be most concerned over the handling of their data (70% and 65% respectively), whilst countries such as Bulgaria, the Netherlands and the Czech Republic are more inclined to state that they are "not at all concerned" (32%, 31% and 30% respectively).[148]

When analysing perceptions of privacy in relation to demographic variables, several points of interest emerge. First, when considering gender, one can find a minor difference between gender and level of concern; women were found to be slightly more concerned about data privacy than men (65% vs. 63%). Second, the younger the respondent, the less concerned they were over the privacy of their data. However, there was one exception to this trend. Those over the age of 55 were not as concerned, and this may be a result of their level of use of technology which would then influence their perception of concern in relation to the privacy of their data. Figure 23 provides a summary of the relationship between age and citizens' perceptions regarding the privacy of their data.

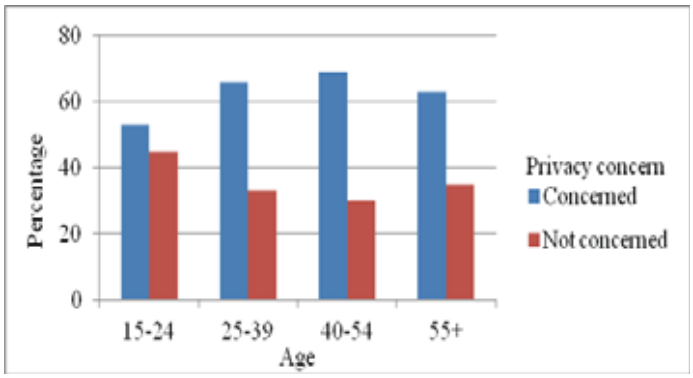


Figure 23: Flash Eurobarometer 225: Citizens perceptions of data protection - age and privacy[149]

In relation to education, the results of the Flash Eurobarometer illustrated a relationship between time spent in education and the level of concern a person may have. Those who had stayed in formal education longer (until the age of 20+) were more concerned about the privacy of their data than those who finished school at the age of 15 (70% vs. 60%). Results also indicated a correlation when considering the occupation of respondents. Those who were not working were less concerned than those who were employees (59% vs. 72%). The survey also considered urbanisation as a demographic factor that could potentially influence perceptions. Results revealed that those in urban areas (such as a town) were less concerned than those in metropolitan and rural areas (62% vs. 66% and 65% respectively).[150]

In addition to exploring public perceptions of the extent of concern over data privacy, the survey also investigated citizens' level of trust in the handling of their privacy by organisations such as medical services, police, banks, insurance companies (to name a few).

[147] Ibid.
[148] Ibid.
[149] Ibid., p. 9.
[150] Ibid.

The survey used the following question for this area of enquiry; the concept of trust was directly mentioned in relation to using material in the "proper way"; however, there was little indication of what the "proper way" constituted:

> I am going to read you a list of (NATIONALITY) organisations that may keep personal information about you. Please tell me if you trust or do not trust each of them to use your personal information in the proper way.[151]

The majority of respondents indicated that they were more likely to trust public organisations such as medical services and doctors (82%), the police (80%) and social security (74%). Trust was lowest amongst private organisations such as mail order companies (24%), travel companies (32%), market and opinion research companies (33%) and credit reference agencies (35%).[152]

When comparing these results across different countries, one finds that the survey revealed that individuals trust in organisations' handling of personal data was higher in some countries than others. For instance, if we take the example of trust in medical services and doctors (see Table 3 below), countries such as Denmark, France and the Netherlands appear to have a higher amount of trust in the handling of their personal data than in Baltic States such as Latvia, and amongst those countries that had recently joined the European Union.

Table 3: Level of trust in medical services and doctors' handling of personal data[153]

Country	Trust in handling of personal data (%)
Denmark	93
France	93
the Netherlands	91
Bulgaria	69
Romania	68
Latvia	63

In relation to private companies, once again differences emerge between different countries. For instance, if we were to consider the example of handling of personal data by mail order companies, levels of trust were higher amongst those in Bulgaria and Cyprus (54% and 50% respectively), but substantially lower in Portugal, Spain and Italy (15%, 14% and 11% respectively). Thus, for both public and private organisations handling personal data, there are noticeable differences based on country and type of organisation handling such data.[154]

When considering demographic variables and their influence on levels of trust in organisations' handling of personal data, the survey revealed noticeable differences in relation to age and education. For example, the older the respondent, the less likely they were to trust any of the organisations referred to in the survey.[155] In relation to travel companies' handling of personal data, levels of trust were significantly lower amongst those aged between 40 and 54, than those aged between 15 and 24 (26.9% vs. 42.5%).[156] The following figure provides further evidence of this:

[151] Ibid., p. 10.
[152] Ibid.
[153] Ibid., p. 11.
[154] Ibid. For further information, see pp. 11-18.
[155] Ibid., p. 19.
[156] Ibid., p. 76.

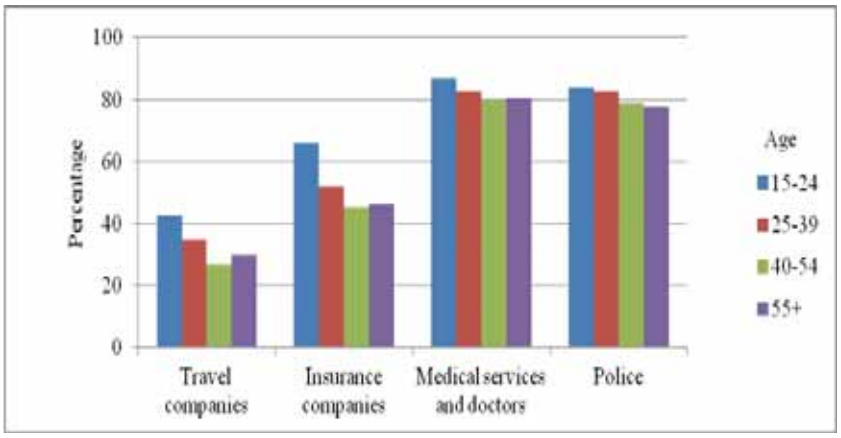


Figure 24: Eurobarometer 225: Age and level of trust in organisations' handling of personal data[157]

Results from the survey revealed that education was another demographic variable that correlated with noticeable differences in respondents' views. In contrast to concern over privacy, those who had spent a longer amount of time in education were more likely to have a higher level of trust in organisations' handling of their personal data. However, in contrast to age, this was not the same across the range of organisations investigated. For instance, respondents indicated higher levels of trust in relation to credit card companies, medical services and doctors; however, those who had finished their education between the age of 16 and 20 had a higher level of trust in mail order and insurance companies than those who had been in education for a longer period of time. Thus, the relationship between level of education and trust is not always clear-cut. The report also indicated a slight difference with regard to occupation, in that those who were self-employed were more likely to be less trusting of organisations' handling of their personal data. For instance, those who were self-employed were less trusting of the police than those who were employees (72.5% vs. 83.2% respectively).[158] In relation to gender and urbanisation, the survey did not find any significant differences.[159]

In addition to measuring privacy and trust, this survey offers an important insight into perceptions of data security on the Internet. The survey used the following question:

> Do you think that transmitting your data over the Internet is sufficiently secure?[160]

With the exception of those who did not use the Internet, for those who did, there was considerable worry by most Europeans (82%) over the security of their data on the Internet in that it was not sufficiently secure.[161] Results were considerably consistent across different EU Member States. With the exception of Denmark, where only 55% of individuals felt their data was not sufficiently secure, the vast majority of individuals (more than 65%) in Europe felt their data was not sufficiently secure.[162]

[157] Ibid.
[158] Ibid.
[159] Ibid.
[160] Ibid., p. 41.
[161] Ibid., p. 40.
[162] Ibid., p. 41.

The survey revealed a slight gender difference in responses concerning the safety of data security on the Internet; 79% of men felt that their data was not secure, compared to 84% of women. In relation to age, public confidence over the security of their data online decreased as respondents increased in age. For instance, 78% of 15-24 years olds stated that their data was not safe, compared to 86% of those who were 55 and over.[163] With regard to education, those who had stayed in education for a longer period of time were more likely to indicate a greater sense of security with regard to their data online; 17% who had been in education until the age of 20+, compared to 8% of those who had left school at the age of 15.[164] As a final point of reference in relation to this question, Gallup found minimal differences with regard to the impact of urbanisation and occupation on citizen views of the security of their data on the Internet.

Relevant to PRISMS, the survey also took steps to understand what measures citizens were taking to enhance their security on the Web. The survey questioned individuals in three phases. First, the survey included a question asking respondents if they had heard of tools or technologies that could improve their data security.

> Have you heard of tools or technologies limiting the collection of personal data from your computer?[165]

Second, researchers asked respondents if they use tools to improve data security.

> Have you ever used these tools or technologies or not?[166]

Lastly, if they had not used them, the survey included a question asking respondents why this was the case.

> If you have heard about these tools and technologies and never used them, what is the most important reason? I will read out some possible reasons, please choose the answer that most applies.[167]

Results revealed that many Europeans (56%) were not aware of tools or technologies that could assist them in securing their data online.[168] For those who had heard of data protection technologies, only 56% had actually used them. For those who did not use them, the report highlighted several reasons for this:

> Around one-fifth of respondents said they weren't convinced that these tools were effective (19%), that they wouldn't know how to use them (19%) or how to install them on a computer (17%), or cited other reasons (17%). [169]

Overall, results point to a lack of understanding of how to select appropriate tools, which subsequently links to there being a lack of sufficient knowledge and understanding of how to operate these tools. Accordingly, individuals were restricted in their ability to take appropriate and efficient measures in both the control and protection of their data online.

---

[163] Ibid.
[164] Ibid.
[165] Ibid., p. 42.
[166] Ibid., p. 43.
[167] Ibid.
[168] Ibid., p. 42.
[169] Ibid.

The authors of the report highlighted the impact of demographic variables on peoples' use of measures to protect their data security on the Internet. For instance, with regard to gender, both awareness and usage of protective measures was significantly lower for women than men. Women were less likely to be aware of relevant data security tools (34% of women vs. 51% of men), and for those who did know about these tools, they were less likely to use them (50% of women vs. 60% of men).[170] The survey revealed similar findings in relation to age, where younger participants were more knowledgeable and more active in their use of tools to help them secure their data on the Internet. For instance, 46% of 15-24-year-olds were aware of relevant technologies compared to 32% of 55-year-olds and above. Education also had an impact of knowledge and awareness; the more time spent in education, the more aware and more active users were. For instance, 24% of those who had left school at 15 were aware of technologies compared to 53% of those who had stayed in school after the age of 20.[171] The field "occupation" also presented researchers with a difference in results in terms of awareness and use of technologies to support users online. For instance, Table 4 (below) demonstrates that those who were self-employed and employees showed greater levels of awareness than those who were in manual labour or not working.

Table 4: Flash Eurobarometer 225: Citizens' perceptions of data protection - occupation and awareness of protective technologies for data security[172]

Occupation	Awareness (%)
Self-employed	50
Employee	47
Manual worker	36
Not working	38

As a final area of interest for PRISMS, this survey also considered the trade-off between surveillance of data and security. The issue of surveillance was presented to individuals in relation to restrictions on privacy and active monitoring of citizens to fight terrorism. Overall, results of the survey suggest that most Europeans are prepared to forego some of their rights to privacy and be confronted with surveillance in the fight against terrorism. However, respondents did feel that it was necessary for authorities to follow clearly defined limits and restrictions; however, this was not a clear-cut "yes" or "no" of support for increasing surveillance in the fight against terrorism. For instance, whilst 75% (overall) felt that people's Internet use should be monitored, there were some limitations: 32% felt that this should be the case only for suspected terrorists, and 18% felt that this should be for suspected terrorists but that it should still be conducted over close supervision of some form of safeguards such as a judge. There were also noticeable differences with regard to the type of surveillance. Europeans seemed to indicate that they were less happy for their credit cards to be placed under surveillance than for their details to be monitored when flying (69% vs. 82%).[173] Monitoring of individuals via different means varied across different countries. For instance, with regard to the monitoring of people's online activities, those in Germany (78%) and Poland (77%) were more likely to approve Internet monitoring than those in Romania (53%).

[170] Ibid., p. 45.
[171] Ibid.
[172] Ibid.
[173] Ibid., p. 49.

The survey did reveal clear patterns in relation to perceptions of surveillance and socio-demographics. For instance, the report indicated that those who objected to the monitoring of personal data with regard to the threat of international terrorism were more likely to be male, higher-educated and self-employed. Those who wanted the complete monitoring of personal data had mostly spent less time in school, were living in rural or urban areas (rather than a metropolitan area) and were manual workers.[174]

4.8.3 *Relationship with other surveys*

This survey highlights several points of interest when comparing and contrasting this survey to other surveys included in this analysis. For instance, as will be discussed at greater length in section 3.6, a comparison between *Eurobarometer 46.1: Information technology and privacy*, published in 1997, and this survey suggests that there has been an increase in privacy concerns amongst citizens in Europe. There is also a difference in the findings of the two surveys in relation to demographics, in that the relationship between education and privacy concerns is now clearer than in 1997. Specifically, the more educated individuals are, the more concerned they may be about the privacy of their data. Furthermore, the inclusion of demographic variables within the Eurobarometer surveys that are assessing privacy have expanded since 1997. In 1997, analysis was restricted to age, gender and education, whereas in 2008, these categories were expanded to also include occupation and urbanisation. Thus, there is a clear indication of researchers trying to further understand the impact of social demographics on privacy concerns.

4.8.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages.

In context of the work being conducted in PRISMS, this Flash Eurobarometer provides us with a clear indication of the growing privacy concerns across Europe. Furthermore, the survey has revealed that there is concern with regard to trusting organisations with the handling of privacy data. Europeans do appear to have some knowledge and awareness of tools that aid the protection of data privacy on the Internet, but this is somewhat lacking in implementation. The survey has also provided an indication of Europeans' attitudes towards surveillance on the Internet; although there is acceptance across the board, there is a concurrent desire for clearly controlled use of surveillance measures. As a final point, in relation to PRISMS, this Flash Eurobarometer provides a useful set of questions to explore public attitudes in relation to privacy, trust and surveillance, and encourages a consideration of what demographic variables the PRISMS survey should include for analysis purposes.

4.9 PERSONLIG INTEGRITET: A COMPARATIVE STUDY OF PERCEPTIONS OF PRIVACY IN PUBLIC SPACES IN SWEDEN AND THE UNITED STATES

Personlig Integritet: A comparative study of perceptions of privacy in public spaces in Sweden and the United States is an academic study by Friedman et al. which was published in

[174] Ibid., p. 54.

the proceedings of the NordiCHI conference, which took place in October 2008.[175] The aim of this survey was to develop an understanding of public views of privacy in public spaces. The survey was a cross-cultural survey that took place in Sweden and the United States. This survey is relevant to PRISMS due to its focus on the issue of how surveillance technologies can impact our sense of privacy in public spaces. It therefore enables a consideration of two of PRISMS' four areas of interest: privacy and surveillance.

4.9.1 *Methodology*

Personlig Integritet: Perceptions of privacy in public spaces took place in two stages. Stage one consisted of a self-completion questionnaire and stage two consisted of face-to-face interviews. In the interest of our analysis of surveys for PRISMS, this analysis focuses on the first part of the study which deals exclusively with the results of the self-completion survey.

In relation to the first stage, researchers recruited participants in public spaces. In Sweden, research staff approached participants sitting in a public space within a university campus. The setting was within the vicinity of a video camera attached to a building that was capturing images of individuals as they walked through the plaza.[176] The Swedish sample consisted of 350 participants, 176 of whom were female, 174 male. The participants were of a mixed age group: 18-25 years (51%) and over the age of 26 (49%). The survey does not provide a more comprehensive categorisation of age as seen in previous surveys (such as the *Flash Eurobarometer 225: Citizens perceptions of data protection)*.[177] Those in the Swedish sample completed a Swedish self-completion survey, where results were later translated into English. Similar to the Swedish survey, the American survey also took place in a university-based setting and researchers recruited participants in the same manner. The United States study consisted of a sample of 250 individuals, 110 males and 140 females. The age range description was limited to those between the age of 18-24 (53%) and 26 and over (47%).[178]

4.9.2 *Main findings*

In an attempt to understand knowledge of the presence of the camera, the first survey question asked whether participants were surprised to find out that there was in fact a camera taking their photograph. In Sweden, there were a substantial number of individuals that appeared to be surprised, with the majority of respondents claiming that they were not aware of the camera (72%).[179] Alternatively, those in the United States seemed to be much more aware of the presence of the camera; only 48% were surprised to learn about the presence of the camera.[180]

Following this question, researchers then asked participants whether they felt the camera was a violation of their privacy: "Do you think this violates your privacy?" Here the concept "privacy" is not defined; rather it is left to the individual to determine what is meant.[181] Results from this question once again indicate a vast difference in perceptions between those

[175] Friedman, Batya, Kristina Hook, Brian Gill, Lina Eidmar, Catherine Sallmander Prien and Rachel Severson, "Personlig Integritet: A Comparative Study of Perceptions of Privacy in Public Spaces in Sweden and the United States", *5th NordiCHI*, Sweden, 2008, pp. 142–151. http://dl.acm.org/citation.cfm?doid=1463160.1463176
[176] Ibid., p. 143.
[177] Ibid.
[178] Ibid., p. 146.
[179] Ibid., p. 144.
[180] Ibid., p. 145.
[181] Ibid.

in Sweden and those in the United States. In Sweden, 47% of respondents felt that the camera violated their privacy, compared to 19% of those in the United States.[182] The survey also enabled results to be measured in relation to gender. Figure 25 demonstrates that in both Sweden and the United States, women were more likely to feel that the camera was a violation of their privacy than men; this difference was more apparent in the United States than Sweden.

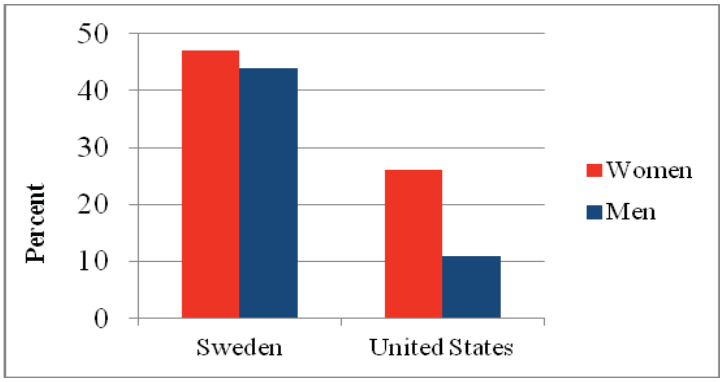


Figure 25: Personlig Integritet: Perceptions of privacy in public spaces - camera as a violation of privacy.[183]

The conference paper did not provide results regarding the impact of age on responses.

The survey then went on to try and further understand the impact of the location of the display of the camera footage, and how this impacted people's feelings about the appropriateness of the location of the display. The survey used the following question:

> The camera displays live video in…
> a…an office with an outside window.
> b...an inside office with no window.
> c…a local apartment.
> d…an apartment in Tokyo.
> e…thousands of local homes.
> f…thousands of homes in Tokyo.
> g…millions of homes across the globe.[184]

However, it was at this point in the research that the surveys used contained slightly different questions. In Sweden, the question did not mention whether the video was "live"; in the United States, some participants were presented with a survey that stated the video was live, whilst others were not. This may have influenced the findings. When asked about the suitability of the location of the cameras' display, those in Sweden were more likely to disapprove of a cameras' display being viewable in public spaces (in other words not in an office), than those residing in the United States. For instance, if the office had an outside window, 35% of those in Sweden thought it was "not all right", compared to 24% in the US.[185] The following figure (Figure 26) provides further evidence of these findings:

[182] Ibid.
[183] Ibid.
[184] Ibid.
[185] Ibid.

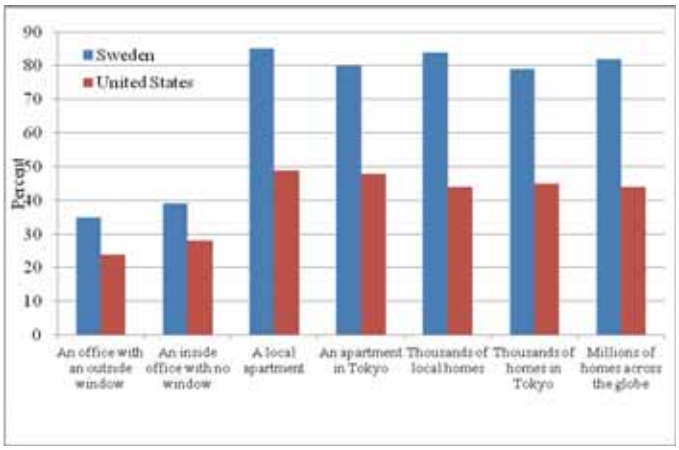


Figure 26: Personlig Integritet: Perceptions of privacy in public spaces - public concerns of camera display in different locations - response - "not all right"[186]

As this figure demonstrates, those in Sweden seemed to be more inclined to dislike the idea of a security cameras display being placed in private sphere, whilst opposition, although present, does not seem to be as strong in the US.

Results from the survey found that women were more likely to have stronger feelings regarding the display of CCTV in private locations being inappropriate. The following figure provides further evidence of these findings:

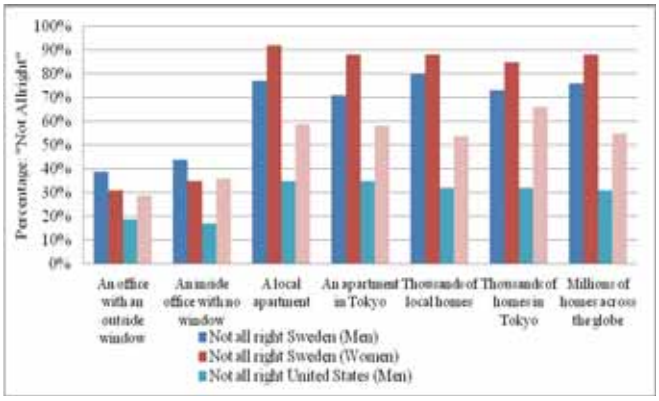


Figure 27: Personlig Integritet: Perceptions of privacy in public spaces - gender and public concerns of camera display in different locations - response - "not all right"[187]

4.9.3 *Relationship with other surveys*

This survey stands out in its attention to focusing on public attitudes towards the display of CCTV systems. Evidence from this survey suggests that individuals prefer the display of CCTV footage to be in a public space rather than a private space. This is somewhat similar to the results of the 2004 *URBANEYE: CCTV in Europe* survey, and the *Two-edged Sword survey* where individuals preferred to have CCTV cameras located in public spaces rather than in private spaces. The surveys included in this analysis point towards both the physical

[186] Ibid.
[187] Ibid.

display of the camera and the location of the camera as important factors in determining public attitudes towards CCTV surveillance systems.

4.9.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages.

Results from this study suggest that there is greater sensitivity towards the positioning of cameras in public spaces and that this has meaning with regard to the violation of an individual's privacy in Sweden than in the United States. This study has also revealed that with regard to gender women in both countries are more likely to perceive cameras in public spaces as a violation of privacy than men. The display of camera footage within the private sphere is also distrusted by those in Sweden, suggesting a desire for greater privacy in relation to where the display of camera footage is located.

4.10 The Globalisation of Personal Data: An International Survey on Privacy and Surveillance

The Globalisation of Personal Data[188] published in 2008, is an international survey that focuses on privacy and surveillance. This project was organised by a team of academics from Queen's University and was funded by the social sciences and humanities research Council of Canada. The survey is particularly relevant to our analysis of public opinion surveys within PRISMS, as it enables us to focus on all four themes: privacy, security, surveillance and trust. In addition, due to the international sampling frame, this survey is particularly useful in gaining a wider understanding of public opinion of privacy and surveillance across the globe. Furthermore the survey also offers an opportunity to understand what measures members of the public are taking enhancing their privacy.

4.10.1 *Methodology*

The survey consisted of a telephone survey that was administered using computer assisted telephone interview technology (CATI). The sample consisted of 9606 respondents from nine countries including: Canada, the USA, France, Spain, Hungary, Mexico, Brazil, China and Japan. Interviews took place in the majority of countries between June and July 2006, in China interviews took place between August and October 2006 and in Japan they took place in December 2007. The sample was designed using a quasi-national sampling strategy to ensure the survey gained a representative sample from each country.[189] The following table provides further information regarding sample sizes from each country:

[188] Chan, Yolande E., Lynda L. Harling Stalker, David Lyon, Andrey Pavlov, Joan Sharpe, Emily Smith, Daniel Trottier and Elia Zurelik, *The Globalization of Personal Data Project: An International Survey on Privacy and Surveillance*, The Surveillance Project, Queen's University, 2008. http://www.sscqueens.org/sites/default/files/2008_Surveillance_Project_International_Survey_Findings_Summary.pdf

[189] Ibid., p. 6.

Table 5: The Globalization of Personal Data - sample information[190]

Country	Sample size
Canada	1001
USA	1000
France	1002
Spain	1000
Hungary	1005
Mexico	1080
Brazil	1000
China	2002
Japan	516

4.10.2 *Main findings*

In order to understand public perceptions of surveillance technologies, the survey designers opted to ask respondents whether they were "very" or "somewhat" knowledgeable about different surveillance technologies, including: the Internet, global positioning systems (GPS), radio frequency identification, closed circuit television (CCTV), biometrics and data mining. From the range of surveillance technologies mentioned, respondents were more likely to be "very knowledgeable" about the Internet (26.8%)[191], and least likely to be "very knowledgeable" about biometrics (2.9%).[192] Those in Canada, the US, France and Spain reported being most knowledgeable about the Internet and other personal location technologies. Those in Mexico and Brazil seem to be the least knowledgeable regarding the range of surveillance technologies listed.[193] Thus, it appears that knowledge of surveillance technologies is not equal across different countries.

In order to try and understand whether people feel as though they have control over their personal information, the survey used the following direct question:

> To what extent do you have a say in what happens to your personal information?[194]

Respondents were given four options to choose from: complete say, a lot of say, some say, no say. When considering results across all countries, the most common response identified was that people felt had complete say over the control of their personal information (39.4%), as opposed to 23.7% who claimed they had "no say".[195] Those who felt as though they had "a lot of say" or "some say", consisted of 15.3% and 19.2% respectively.[196] Those in Canada, Mexico, Spain, and the USA were more likely to believe that they had complete say than those in China and Japan.

In relation to control over personal information individuals, researchers also asked respondents about the various actions that they had chosen to take to help protect their personal information. Researchers asked the following question in relation to 10 different measures:

---

[190] Ibid.
[191] Ibid., p. 8.
[192] Ibid., p. 9.
[193] Ibid., p. 8.
[194] Ibid., p.12.
[195] Ibid.
[196] Ibid.

Have you ever done the following for the purpose of protecting your personal information?"[197]

The following table (Table 6) provides further information regarding the various measures participants would be inclined to take to protect their personal information:

Table 6: Globalisation of Personal Data - measures taken to enhance protection of personal information[198]

Measure	Percentage
Refused to give information to the business	51.5%
Refused to give information to government agency	20.4%
Asked company to remove you from marketing list	33.6%
Asked company not to sell info to another company	35.6%
Ask business about policies on collection of consumer information	17.6%
Ask company to see what personal info they had in records	12.0%
Purposefully gave incorrect information to mocked	15.3%
Purposefully gave incorrect information to government agency	4.2%
Read online privacy policies on website were making purchases	33.2%
Read online privacy policies on government website	24.2%

Results from the survey found that of the 10 measures, responders were most likely to have refused to give their information to a business (51.5%).[199] Respondents were least likely to have purposefully given incorrect information to government agency (4.2%).[200] Furthermore, in general, respondents were more likely to take protective measures in relation to consumer related activity rather than activities relating to the government. Overall findings from this survey suggest that Canadians and Americans appear to be more protective of their personal information than individuals in other countries.[201]

The survey also sought to understand the amount of trust afforded by members of the public towards governments and private companies regarding whether they felt they were able to do an appropriate job of protecting their personal information. The survey used the following question to understand whether governments could be trusted to protect individual rights towards privacy when trying to ensure national security:

> When it comes to the privacy of personal information, what level of trust you have that your government is striking the right balance between national security and individual rights.[202]

Respondents were given two options to choose from: "very high" or "reasonably high". Of all the participants within the survey, 31.7% selected the option of "reasonably high", whilst only 5.5% stated that they had very high trust in the government, 62.8% of the sample did not select either response.[203] With regard to those selecting "very high" those in Hungary, USA and China (11.4%, 9.9% and 9.7% respectively) appear to be more trusting than those in

[197] Ibid., p.14.
[198] Ibid., pp. 14-15.
[199] Ibid., p. 14.
[200] Ibid., p. 15.
[201] Ibid., p.14.
[202] Ibid., p. 13.
[203] Ibid.

Japan and Brazil (0% and 2.7% respectively).[204] These results suggest that a substantial number of individuals do not hold much (if any) regard towards trusting their governments in being able to appropriately handle and protect their personal information.

Researchers also asked respondents whether they trusted private companies with protecting their personal information:

> What level of trust do you have that private companies, such as banks, credit card companies and places where you shop, will protect your personal information?[205]

As with trust in the government, trust in private companies by members of the public seems to be absent, with 55.3% of respondents not selecting either "very high" or "reasonably high".[206] Respondents were more likely to express that they had a "reasonably high" level of trust towards private companies than a "very high" level of trust (37.4% compared to 7.3%).[207] When comparing results across different countries, those in Hungary were more likely to have a very high level of trust in private companies than those in Japan (14.7% compared to 1.4%).[208]

The survey also asked respondents whether they were worried about providing personal information on the Internet. In the following question, the survey gave respondents a selection of types of personal information to consider in relation to the question being asked:

> When it comes to privacy, how worried are you about providing personal information on websites, such as your name, address, date of birth, gender?"[209]

The survey gave respondents four options to choose from: "very worried", "somewhat worried", "not very worried" and "not worried at all". When considering results from all countries respondents were most likely to indicate that they were "somewhat worried" about providing personal information websites and what this meant that privacy (37.2%). Across all countries respondents were least likely to indicate that they were "not worried at all" (15%).[210] Those living in Brazil and Spain appear to be most concerned with providing personal information on the Internet (59.7% and 32% respectively).[211] Those living in Hungary and France seem to be least concerned with providing personal information on the Internet (28.4% and 24.5% respectively).[212]

The survey also made a concerted effort to try and understand the relationship between security and what enhanced security measures implied for a person's privacy. The researchers used the following question to try and gauge public opinion regarding this matter:

---

[204] Ibid.
[205] Ibid.
[206] Ibid.
[207] Ibid.
[208] Ibid.
[209] Ibid., p. 20.
[210] Ibid.
[211] Ibid.
[212] Ibid.

> The government of __ has enacted laws aimed at protecting national security. To what extent do you believe laws aimed at protecting national security or intrusive upon personal privacy?[213]

Once again the survey provided respondents four options to choose from: highly intrusive, somewhat intrusive, not very intrusive and not intrusive at all. Within all countries respondents were most likely to indicate that they felt the laws aimed at protecting national security were somewhat intrusive upon their own privacy (37.8%); only 10.6% felt that it was not intrusive at all. Differences in results emerge across countries; those in China, for instance, were more likely to claim that laws to improve national security were not very intrusive upon their personal privacy (50%).[214]

The survey also asked respondents about their perceptions of the effectiveness of CCTV in different areas:

> Some communities and private companies are using surveillance cameras, also known as closed circuit televisions or CCTVs is, to monitor public places in order to deter crime and assist in the prosecution of offenders. In your opinion, how effective are the following CCTVs in reducing crime?[215]

Respondents were most likely to indicate that they felt in-store CCTV was "very effective" (33.9%) as opposed to community CCTV (26.5%).[216] Community CCTV was seen to be most effective in countries such as Brazil (42.9%) and Mexico (38.2%). As with community CCTV, in-store CCTV was seen to be more effective in Mexico (53.2%) and Brazil (51.7%).[217]

4.10.3 *Relationship with other surveys*

This survey has revealed similar findings to the *Flash Eurobarometer #225*, also conducted in 2008, in which respondents claimed to be concerned about the privacy of their personal information online. The two surveys also identified public support towards the presence of surveillance technologies to enhance security. Both surveys also reported identical findings with regard to the trusting of public organisations over private organisations in the handling of personal data.

4.10.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages.

The Globalization of Personal Data project by Queen's University offers an insight into a cross-cultural analysis of public opinion regarding privacy, security, surveillance and trust of governments and private companies with personal information. The survey revealed that there are fundamental differences between those who believe that they have control over their personal information and those who do not. Some individuals appear to have been making a

[213] Ibid., p. 28.
[214] Ibid., p. 26.
[215] Ibid., p. 29.
[216] Ibid.
[217] Ibid.

concerted effort to maintain control over their personal information by taking several measures, however this is not consistent, nor is it very are widespread across all countries. Individuals appear to be concerned with trusting both governments and private companies with the job of taking care of their personal information. Many members of the public that participated in the survey do not seem to hold a very positive perception of the impact of CCTV surveillance technologies on security. Overall this survey has found that knowledge and perceptions of the privacy and surveillance in digital era are somewhat negative.

4.11 CANADIANS AND PRIVACY

Canadians and Privacy[218] is the final report of a study conducted by EKOS Research Associates Inc. on behalf of The Office of the Privacy Commissioner of Canada (OPC). The report was published in March 2009 and presents findings from a survey of Canadian individuals that aimed to explore public understanding of privacy issues, legislation and federal privacy institutions.[219] This survey is relevant to PRISMS because it touches on all four areas of interest: privacy, security, trust and surveillance. In addition, the survey provides an opportunity to not only understand what measures individuals might be taking to enhance their privacy, but also how they rank their own abilities to protect their personal data.

4.11.1 *Methodology*

The *Canadians and Privacy* study was a telephone survey of a random sample of 2,028 Canadians over the age of 16. The survey, carried out by EKOS Research Associates Inc., was conducted between the 23 February and the 9 March 2009.[220]

4.11.2 *Main findings*

In order to understand how individuals felt about privacy online researchers asked respondents how they felt they handled protecting their privacy and their personal information. Researchers used the following question to gauge this, in which respondents were able to rate their own behaviour from "very poor" to "very good":

> In your day to day life, how good of a job would you say you are doing to protect the privacy of your own personal information?[221]

Responses to this question suggest that the majority (56%) of respondents believed they were "good" at protecting their own personal information online. Other responses ranged from "very good" (20%), to "neither" (17%). A small minority of individuals indicated that they were doing a poor job of protecting their own privacy (poor – 5%; very poor – 1%).[222] The report was able to show how this question has been answered over time; between 2006 and 2009 people believed themselves to be "better" at taking care of their own privacy online.[223]

---

[218] EKOS Research Associated Inc., *Canadians and Privacy: Final Report*, March 2009. http://www.priv.gc.ca/information/por-rop/2009/ekos_2009_01_e.asp
[219] Ibid., p. iii.
[220] Ibid., p. 1.
[221] Ibid., p. 7.
[222] Ibid.
[223] Ibid.

Those who were over the age of 65 felt particularly strongly about their ability to manage their own personal information.[224]

The survey used the following question to further understand public attitudes towards what they believed to be the "most important issue" to face Canada in the foreseeable future:

> Please indicate the extent to which you agree or disagree with the following statements:
> - Protecting the personal information of Canadians will be one of the most important issues facing our country in the next ten years.
> - I am concerned that our current focus on security following the 9/11 terrorist attacks will unnecessarily restrict the privacy and civil liberties of Canadians.
> - I am confident that businesses and organizations have adequate security safeguards to protect my personal information.[225]

Of the three statements, respondents were more likely to agree (62%) with the first statement that protecting citizens personal information is likely to be one of the most important issues facing Canada in the next 10 years; only 19% disagreed. Respondents were most likely to disagree (44%) with the third statement, displaying distrust towards businesses and organisations abilities to protect their personal information; only 34% felt they would be able to protect their information. With regard to socio-demographic influences on these perceptions, those with higher education levels were more distrustful of businesses and organisation regarding the handling of their personal data.[226] Younger participants were more inclined to believe that businesses and organisations could be trusted with their personal data (47% of those under the age of 25 vs. 27% of those aged 45 to 64).[227] In relation to the second statement, 47% agreed that current focus on security following 9/11 had the potential to restrict privacy and civil liberties; 29% disagreed and 22% responded with "neither".[228]

In relation to concern over privacy, the survey sought to understand whether individuals were confident about the effect of new technologies on the privacy of their data. The final report reveals changes over time in whether the public believe they have enough information to know how new technologies might affect their personal privacy: of those that agree that they have enough information, there was a slight increase between 2000 and 2003 (from 50% of people who felt they had enough information to 54%). Between 2003 and 2005 there is evidence of a decrease in people thinking they have adequate knowledge of how new technologies affect their personal privacy (from 54% to 47%). There was a slight increase between 2004 and 2007 in the percentage of people that felt they had enough information to understand how new technologies affected their personal privacy (from 47% to 51%). From 2007 to 2009, there was yet another decease in the percentage of people that felt they understood how new technologies affected their personal privacy (from 51% to 45%).[229] Figure 28 demonstrates further evidence of these trends:

[224] Ibid.
[225] Ibid., p. 8.
[226] Ibid.
[227] Ibid.
[228] Ibid.
[229] Ibid., p. 14

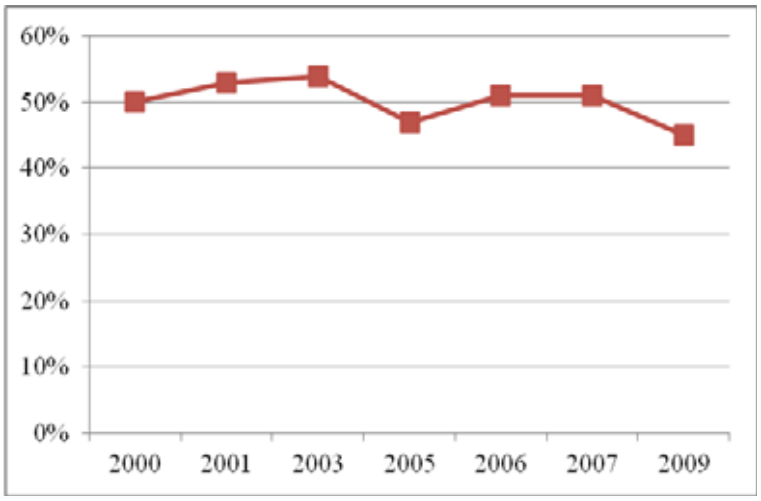


Figure 28: Canadians and Privacy - percentage of people that agree they have enough information to know how new technologies might affect their personal privacy[230]

The survey then asked respondents the extent of their concern over the impact of new technologies on their privacy. Participants were most likely to claim they were "somewhat concerned" (48%), 42% claimed they were "very concerned", 9% argued they were "not concerned" and 1% did not know or did not reply.[231] Men were more likely (11%) than women (6%) to declare that they were not concerned. In relation to age, those between the age of 45 and 64 were more likely to be concerned than younger participants.[232]

The survey identified the following results in relation to what "new technologies" people were most concerned:

Table 7: New technologies and privacy concerns[233]

New technology	Concern
Internet/Computer Use	26%
Hacking technologies/invasion of privacy/identity theft	10%
Credit cards/debit card concerns of transactions	5%
Surveillance/tracking/recording technologies	5%
Banking/Online banking	3%
Use of cell phone/telecommunication technology	3%
Online social networking sites	2%
DK/NR	45%

Respondents appeared to be most concerned with the Internet and use of a computer (26%), this was following by hacking technologies (10%), surveillance technologies (5%) and concerns over financial transactions online (5%). Respondents seemed to be less concerned about communication devices and social networking sites. A significant number of respondents indicated that they "didn't know or did not respond" to the question (45%),

[230] Ibid.
[231] Ibid., p. 15.
[232] Ibid.
[233] Ibid., p. 16.

although reasons for this were not given.[234] Older respondents (those aged between 45 and 64) are more likely to be concerned about the use of the Internet/Computer than younger uses (30% vs. 16%).

In relation to use of the Internet, researchers asked respondents to rate their ability to protect themselves online:

> How would you rate your ability to take the appropriate precautions to protect your personal information and ensure that using the Internet is as safe and secure as possible?[235]

The majority of respondents indicated that they were very good at protecting themselves (54%), 15% felt they were very poor at protecting themselves, 24% stated neither and 6% either stated they did not know or did not respond to the question. Thus, there appears to be mixed feelings with regard to the abilities of individuals to protect themselves online. From a socio-demographic perspective, younger respondents seemed to be more confident than older respondents, as did those who were more educated.[236]

Following questions about privacy and new technologies, researchers asked respondents a series of questions in relation to their awareness of, and attitudes towards, surveillance technologies. For instance, when asked about their awareness of radio frequency identification tags (RFID), the majority of respondents (64%) were not aware of them.[237] Men were more likely than women to have heard of them.[238] When asked about whether they were concerned about the impact of this form of new technology on their privacy, 44% of respondents indicated they were "somewhat concerned" and 38% claimed they were "very concerned".[239] In particular, older participants, and men were more concerned.[240] In contrast, respondents seemed to be more aware of nanotechnology than of RFID, with 45% claiming they had "definitely" heard of nanotechnology and 43% of participants claiming they had "maybe" heard of nanotechnology.[241] In relation to concern over nanotechnology, as with RFID, high proportions of respondents indicated that they were either "somewhat concerned" or "very concerned" (42% and 41% respectively).[242] Thus, when it comes to surveillance and its impact on concern over privacy, there appears to be a high proportion of individuals who show concerns.

The survey also sought to investigate the trade-off between privacy and security. Researchers asked participants about this in an indirect fashion. First, they asked participants whether governments should consider the importance of a person's privacy in relation to their supplying law enforcement agencies with enhanced powers. The majority of respondents indicated that this was either "somewhat important" (45%) or "very important" (45%). Only 7% indicated that this was "not important".[243] Thus, for some, privacy is an important consideration when increasing the powers of law enforcement agencies. When it came to asking about "trust" of the protection of their privacy in relation to law enforcement agencies,

[234] Ibid.
[235] Ibid., p. 17.
[236] Ibid.
[237] Ibid., p. 18.
[238] Ibid.
[239] Ibid., p. 19.
[240] Ibid.
[241] Ibid., p. 21.
[242] Ibid., p. 20.
[243] Ibid., p. 25.

the majority of respondents indicated that they were "moderately confident" that law enforcement agencies adhere to privacy laws (66%). Fifteen per cent indicated they were "very confident" and 17% stated they were "not confident".[244] Thus, some individuals are not entirely trusting of law enforcement agencies' ability to protect their privacy.

The survey also included questions that sought to identify the various measures individuals were taking to ensure their privacy. When asked whether they had taken any action to protect their personal information, the majority of respondents claimed that they had declined to share their personal information with businesses (51%). Respondents were least likely to request to see personal information that is being kept by the government (10%).[245] The survey also asked respondents whether they had taken certain measures to protect their passwords. The majority of respondents indicated they had used passwords that contained random letters and that would then be difficult to guess (65%). Fifty-eight per cent stated they would look for a padlock symbol that would then indicate that they are using the secure site. Forty-three per cent of the sample indicated that they did not use passwords to protect their information on a digital portable device.[246] From a socio-demographic perspective, those who had been in education for the longest were particularly likely to use passwords that would be difficult to guess. In addition, men were more likely to protect their passwords on digital portable devices than women.[247] Thus it seems that whilst respondents are trying to protect their privacy online they do not necessarily always take measures that are available to them.

4.11.3 *Relationship with other surveys*

As with other surveys, namely *The Globalisation of Personal Data,* this survey demonstrates that Canadians do show some level of concern with regard to the privacy of their personal data. Likewise, as seen with other surveys analysed here, such as the *Flash Eurobarometer #225: citizens perceptions of data protection,* some individuals are taking some measures to enhance their privacy on the Internet.

4.11.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages.

Overall this survey has found individuals are concerned with the impact of both existing and new technologies on their privacy. Specifically, respondents mentioned concerns around the way their personal data is vulnerable on the Internet, and the ways in which new technologies, specifically nanotechnologies or RFID technology might impact upon their privacy. This study has also revealed that some respondents believe they did a "good job" at protecting their own personal information online. Many respondents expressed confidence that law enforcement agencies would respect privacy laws in the handling of their personal data; however, there are some that do not necessarily trust law enforcement agencies ability to protect their personal privacy.

[244] Ibid., p. 27.
[245] Ibid., p. 29.
[246] Ibid., p.31.
[247] Ibid.

4.12 PRIVACY 2.0: PERSONAL AND CONSUMER PROTECTION IN THE NEW MEDIA REALITY

Privacy 2.0: personal and consumer protection in the new media reality[248], published in November 2009, was conducted by Bradtzaeg and Luders of SINTEF (an independent research organisation in Norway) on behalf of the Norwegian Consumer Council. The survey was fed into other SINTEF projects; NETPOWER, RECORD and VERDIKT under Norway's research program for ICT. The aim of the study was to develop a wider understanding of the use of social media and the various challenges of this use for consumers in relation to their privacy.

4.12.1 *Methodology*

The study was comprised of five different aspects, ranging from a survey to interviews with different parties and document analysis. For the purpose of PRISMS, our attention will be on the outcome of the survey concerning Norwegian Internet users.[249] The survey is part of a longitudinal study that took place over a period of three years. The first round of the survey took place between May and June 2008. During this round, 2000 participants took part in an online survey that was distributed via e-mail. The second round took place a year later, between May and June 2009. During this stage, 1,372 individuals from the first round took part in a second online survey. As identified in the report, the reduction in responses is typical of longitudinal studies. Researchers involved in writing the report claimed that the same "should be more-or-less nationally representative of Internet users in Norway".[250] Unfortunately, Brandtzaeg et al. did not include a copy of the questions they used in the survey in the report.

4.12.2 *Main findings*

Prior to understanding public perceptions of privacy in relation to social networking sites, the survey sought to explore how social networking sites are being used by Norwegians. Findings from this survey suggest that over time the use of social networking websites has increased (from 53% in 2008, to 66% in 2009).[251] Results from the survey suggest that the most popular social networking sites in Norway are: YouTube, Wikipedia and Facebook.[252] Women were more likely to use social networking sites for "social" reasons; alternatively, men were more instrumental and information-seeking in their use of social networking sties. For instance, with regard to Wikipedia 35% of men use the site compared to 21% of women. Alternatively, when considering the use of Facebook, women were more likely to be accessing the site on a daily basis than men (35% compared to 21%).[253] In relation to age, the 2009 survey finds that those aged 15 to 30 are the most active users of social networking sites. Generally speaking the older respondents were the less they used social networking sites (although there was an increase in use for all ages between 2008 and 2009). For instance, 96% of 15-30 year olds used social networking sites in 2009 compared to approximately 25% of those between the age of 61 and 75.[254]

[248] Brandtzaeg, Bae and Luders, 2009.
[249] Ibid., See Chapter 4 of the report.
[250] Ibid., p. 37.
[251] Ibid., p. 38.
[252] Ibid., p. 39.
[253] Ibid., p. 40.
[254] Ibid., p. 39.

Knowing that individuals are actively using social networking sites enables us to contextualise information that has the potential to impact attitudes and actions towards the privacy of personal data. A second line of questioning within the survey saw researchers asking respondents about their openness to the sharing of personal data via social media. Results reveal that there were some respondents that appeared to be apprehensive with regard to sharing information on social networking sites and what this implied for personal privacy. Over the course of a year, there was a 1% increase in respondents stating that they do not participate in social networking sties due to fear of the abuse of their personal data (14% in total, 2009).[255] Across the different age groups, 50% of younger users "disagreed/disagreed strongly" with the statement: "It is very likely that I will share my personal information on the Internet in the future", 30% of those aged 15 to 30 claimed they "disagree/strongly disagree".[256] The survey revealed that 28% of respondents indicated that the profiles they had on social networking sites were "open", unfortunately, Brandtzaeg et al. did not supply information (as with previous surveys) about the different levels of privacy settings that users had set.

In an attempt to understand people's actions in monitoring how their personal data is used, this survey asked respondents several questions. When asked whether individuals were likely to read privacy related terms and conditions before accepting them, results suggest the younger the respondent, the less likely they were to read terms and conditions.[257] When the researchers asked whether all respondents that used social networking sites felt that the social networking sites they used most often would be able to protect their privacy, 64% claimed they believed they would be able to protect their privacy. [258] This trust in social networking sites was further emphasised when 36% of all respondents using social networking sites indicated they "disagree/disagree strongly" with the claim "I am confident that it is safe to share personal content with others on the social networking site I use most often".[259] Interestingly, despite these findings that indicate trust towards social networking sites, 58% of respondents claimed they had "lost control over how personal information is collected and used by commercial companies". A social networking site, which respondents appear to trust, would be a "commercial company". Further information as to what commercial companies' individuals feel they have lost control to could have been an interesting addition to this survey.

4.12.3 *Relationship with other surveys*

This survey has revealed similar findings to the survey conducted by the *PEW Research and American Life Project: Digital Footprints*, from 2006, in that there is a degree of concern relating to the privacy of personal data online. Specifically, individuals in both surveys report feeling that they have lost control of how their personal data is used online. However, a number of survey in this analysis [e.g., *The Globalization of Personal Data* (2008), and the *Special Eurobarometer #359: Data protection and e-Identity* (2011)] indicate that this does not necessarily translate into action in relation to trying to maintain control over data.

[255] Ibid p. 45. Note: The degree of confidence for the survey's results were not included, thus it is not known whether this is a significant increase of not.
[256] Ibid.
[257] Ibid., p. 46.
[258] Ibid.
[259] Ibid., p. 47.

4.12.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages.

Findings from this survey suggest that some respondents are hesitant about sharing personal information on the Internet. The survey also highlighted the contrasting gap between people being concerned about the privacy of their information, and action taken by individuals to enhance the privacy of the personal data online. A further gap was revealed by the survey, specifically, that many individuals report they have lost control over how their personal information is collected and used by commercial companies on the Internet. Yet, many respondents seem to indicate that they trust private social networking providers to be able to fulfil the task of protecting their privacy.

4.13 STATE OF THE NATION SURVEY

The *State of the Nation Survey*[260] was published in February 2010. The survey of British individuals was conducted by ICM and commissioned by the Joseph Rowntree Reform Trust. The survey covers a range of topics including public opinion regarding British government and the actions taken by the government, public opinion on government policies, questions concerning a proposed Bill of Rights, perceptions of surveillance technologies and individuals' political identities. This survey provides an understanding of British public opinion towards privacy, surveillance, trust and security.

4.13.1 *Methodology*

The *State of the Nation Survey* by ICM involved face-to-face interviews that took place in public spaces (the street) between 20 January and the 7 February 2010. The sample consisted of 2288 British residents over the age of 18. ICM considered this quota sample to be a representative sample that they weighted by age, gender, work status, housing tenure and region.[261] Unfortunately, ICM did not provide information as to the breakdown of these results according to socio-demographic variables; a clear limitation to the study in relation to the secondary analysis of findings.

4.13.2 *Main findings*

Discussions regarding British public opinion surrounding what should be included in a proposed Bill of Rights provide us with an indication of how interested British people are about having a right to privacy. ICM used the following question to gain insights of what members of the public thought should be included under the proposed Bill of Rights:

> I would now like to ask you some questions about a Bill of Rights, which some people have been talking about. On this card is a list of rights that some people have said should be

[260] The Joseph Rowntree Reform Trust Ltd. and ICM, *State of the Nation 2010 Poll*, 20 March 2010. http://www.jrrt.org.uk/publications/state-nation-2010-poll

[261] Ibid., p. 1. Note: No indication was given as to where in the UK the face-to-face interviews took place.

> included in a Bill of Rights. I'd like you to go through the list and tell me, which, if any, you yourself think should be INCLUDED in a Bill of Rights.[262]

In relation to privacy, individuals believe they should have a right to know what information government departments hold about them (81%) and that they should have a right to privacy on their phone, mail and e-mail (79%).[263] These results suggest that individuals do care about the privacy of their communication related activities as well as the information that is held about them by government departments.

The survey included a second question relating to the issue of privacy concerns, by querying whether respondents think that various government proposals for handling personal information is a "good idea" or "bad idea":

> From what you have seen or heard do you think the following government proposals for handling personal information are a good idea or a bad idea?[264]

Respondents' answers to this question suggest a general distrust of government proposals for handling their personal information. More specifically, when asked whether personal information should be stored on a large computer system and shared across government departments, 34% felt this was a "very bad idea", while only 6% indicated that it was a "very good idea". ICM identified similar findings with regard to holding all medical records on a centralised computer system, with 29% indicated it is a "very bad idea" and 13% indicated it was a "very good idea". Government access to phone, e-mail and Internet browsing records saw even greater opposition with 55% of respondents thinking it was a "very bad idea" and 3% of respondents thinking it was a "very good idea".[265] Accordingly, there does not seem to be much support for government access to personal information nor is there much confidence in government ability to handle personal data.

The survey also provides an important indication of public attitudes towards surveillance technologies. For instance, ICM asked individuals about their opinion of whether they felt that the introduction of an ID card would be a "good idea" or a "bad idea":

> The government has proposed the introduction of identity cards that, in combination with your passport, will cost around £93. From what you have seen or heard do you think that this proposal is a good idea or a bad idea?[266]

The majority of respondents indicated that this was a "bad idea" (27% felt it was a "very bad idea" and 25% felt it was a "bad idea"). Only 10% felt that it was "very good idea", and 27% felt that it was a "good idea".[267] Support for a national ID card that would enhance surveillance over individuals does not seem to be supported at the time of the survey. The wording of the question, specifically the inclusion of monetary costing involved in a national ID card, may have impacted the responses given by participants. Due to the ambiguous question wording and the mention of the cost, it is unclear whether respondents believe that a national ID card is a good or bad "idea". In this instance, respondents could be opposed to the cost of an ID card, not necessarily the ID card itself. In future, survey designers should try to

[262] Ibid., p. 5.
[263] Ibid.
[264] Ibid., p. 6.
[265] Ibid.
[266] Ibid.
[267] Ibid.

avoid any leading or unclear questions to ensure that the question answered is directly related to the area of interest.

In addition to asking respondents about their views of surveillance technologies in the form of national ID cards, ICM asked respondents about the use of DNA in relation to security and preventing and solving crime. Researchers used the following question to understand whether participants felt it was appropriate for DNA to be permanently kept on file. Researchers presented respondents with three statements (relating to an individual having committed a criminal act) and asked them whether DNA should be kept permanently or kept for a set period of time:

> In England and Wales, the police can currently take a DNA sample from anyone arrested for a recordable offence before they are charged with an offence. This sample is analysed to produce a DNA profile which is kept permanently on a database, whether or not the person is convicted or even charged with an offence. For each of the following please tell me whether you think the police should keep a person's DNA profile on the database permanently, or whether there should be a time limit.[268]

Respondents were more likely to state that DNA should be kept permanently for those who have been convicted of violent crimes, such as murder or rape (90%), or burglary (57%). Respondents were more likely to indicate that DNA should be kept for certain amount time in relation to acts such as being drunk and disorderly (65%).[269] Thus, the greater the threat to security, the more respondents were likely to agree a permanent surveillance measures should be taken.

The final question used in the survey that is of interest to PRISMS relates to the handling of personal data by the police:

> I am now going to read out a number of policies and proposals, and I would like you to tell me to what extent you support or oppose each?[270]

The four policies and proposals consisted of:

1. Allowing the police to take a DNA sample from a person before they are charged with an offence.
2. Allowing the police to keep a person's DNA profile on a database permanently, even if they are never charged or convicted of an offence.
3. Allowing the police to keep a person's DNA profile on a database for six years, even if they are never charged or convicted of an offence.
4. Allowing the police to keep a person's record of arrest permanently, even if they are never charged or convicted of an offence.

ICM presented respondents with six options to choose from: "strongly support", "tend to support", "neither support nor oppose", "strongly oppose" or "don't know". With regard to the first policy relating to the police being able to take DNA from a person before they are charged, respondents were most likely to "strongly oppose" (31%) the policy, rather than "strongly support" (17%) the policy. Likewise, with regard to the second item, respondents were most likely to "strongly oppose" (41%) than "strongly support" (14%) the proposal of

[268] Ibid.
[269] Ibid.
[270] Ibid., p. 7.

the police being able to keep a person's DNA profile on a database permanently even if they had never been charged or convicted. The third proposal, "allowing the police to keep a person's DNA profile on a database for six years, even if they are never charged or convicted of an offence" also received a negative response. Those that "strongly opposed" the measure consisted of 37% of the sample, and those that "strongly" supported the measure consisted of only 14%. The final measure, which did not involve the police keeping a person's DNA, but did involve permanently keeping note of a person's arrest even though they had not been charged or convicted also received a great deal of opposition: 37% "strongly opposed" the proposal, and 11% "strongly supported" the proposal.[271] Thus, results suggest that individuals are predominantly against police keeping DNA records of those who are not charged or convicted of an offence, thereby showing a desire to maintain an individual's privacy.

4.13.3 *Relationship with other surveys*

As revealed in this survey as well as the *Flash Eurobarometer #225*, some individuals feel they have the right to know what information governments hold about them. Yet, there is a noticeable difference between this survey and other surveys included in this analysis in with the level of trust individuals have over their government's ability to appropriately handle their personal data. Results from this survey support other survey's findings (such as *A survey on EU citizens' trust in ID Systems and Authorities)* where researchers identified that those residing in the UK were more sceptical towards authorities handling of personal data. The lack of trust in organisations abilities to manage personal data has also been observed in other surveys (not included in this analysis), for instance, a study in 2010 commissioned by the Information Commissions Office in the UK, found that 92% of individuals were concerned about how their information was handled and furthermore, 60% felt they had lost control of how their personal information is kept and processed.[272] However, this survey does not provide an opportunity to assess whether citizens would be more trusting of private organisations than governments. Also, like other surveys, the use of surveillance technologies to monitor communication that focus on the body, such as DNA, generate more opposition than other technologies such as CCTV.

4.13.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages.

The findings from the survey suggest that privacy is particularly important to individuals in relation to their basic human rights within the UK. In addition individuals appear to have a desire to maintain their privacy in relation to technologies that enhance surveillance with the aim of achieving greater security. The survey has also revealed that citizens lack trust in the British government's ability to look after personal data.

---

[271] Ibid.

[272] SMSR: Social and Market Strategic Research, *Report on the Findings of the Information Commissioner's Office Annual Track 2010*, Information Commissioners Office, November 2010. http://www.ico.gov.uk/about_us/research/~/media/documents/library/Corporate/Research_and_reports/annual_track_2010_individuals.ashx

4.14 FINANCIAL TIMES/HARRIS POLL: BODY SCANNERS

Results of a poll conducted by the *Financial Times/Harris Poll: Body Scanners* were released in March 2010.[273] The purpose of the poll was to develop an understanding of public attitudes towards increased security measures at airports following the attempted bombing of a plane headed for the USA on Christmas Day. This survey is relevant to our work on PRISMS, because it allows for the consideration of the continual trade-off between surveillance and security in the digital era.

4.14.1 *Methodology*

The Financial Time/Harris Poll consisted on an online opinion survey, conducted by Harris Interactive, a global market research company. The poll took placed between the 3 and 10 February 2010. The sample of 7,256 individual's consisted of participants from seven countries: the United States, Great Britain, France, Italy, Spain, Germany and China.[274] The authors of the report, Harris Interactive, did not include details regarding the selection procedure for participants. Harris Interactive did, however, include a point of reference to show that they did apply weighting to the sample to reflect the wider population of each country. The following table (Table 8) supplies further information regarding the nature of the sample:

Table 8: Financial Time/Harris Poll: Body scanners - sample information[275]

Country	Sample size	Age group
United States	1006	16-64
Great Britain	1097	16-64
Spain	1019	16-64
France	1093	16-64
Germany	1016	16-64
Italy	1004	18-64
China	1021	18-64

4.14.2 *Main findings*

This survey includes three relevant questions relevant to our understanding of the trade-off between surveillance and security in PRISMS. Harris Interactive asked respondents whether following the failed plane bomb plot they thought that security should be enhanced at airports with the use of full body scanners. In the following question, the researcher framed the issue of security with the use of examples, and they introduced "surveillance" with the use of specific surveillance technologies:

> Following the failed attempt to explode a bomb on a plane in America on Christmas day, certain measures to increase not only airline security, but also security measures in other locations, are being discussed. How much do you agree or disagree with the following

[273] Harris Interactive, *Most Adults in Largest European Countries, U.S. and China Agree Full Body Scanners Should Be Introduced in Airports*, 3 March 2010.
http://www.harrisinteractive.com/vault/HI_FinancialTimes_HarrisPoll_March_2010_02.pdf
[274] Ibid., p.3.
[275] Ibid.

> statements about some of these measures?' 1. Body scanners that X-ray the full body should be introduced at airports.[276]

In all countries, researchers found that respondents were more likely to agree with the statement than disagree. The following figure supplies further information regarding these results:

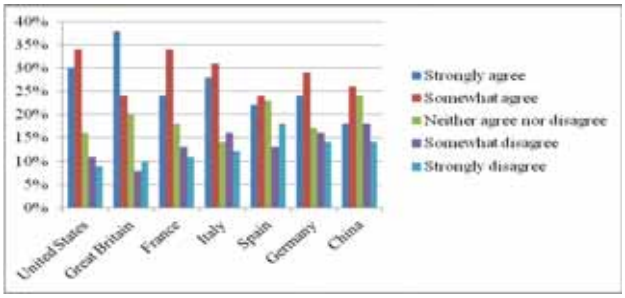


Figure 29: Financial Times/Harris Poll: Body scanners - body scanners "should" be introduced at airport security[277]

Harris Interactive were able to identify differences in responses to this question across different countries. Those more likely to "strongly agree" were from Great Britain (38%), the United States (30%) and Italy (28%). Those who were more likely to "strongly disagree" were from China (18%), Germany (16%) and Italy (16%). Researchers identified a substantial percentage of individual's from China (24%), Spain (23%) and Great Britain (20%) who neither agreed nor disagreed with the introduction of full body scanners at airports to enhance security.[278]

Harris Interactive use the following question to determine whether respondents felt that security checks by governments should be increased in public spaces:

> Following the failed attempt to explode a bomb on a plane in America on Christmas day, certain measures to increase not only airline security, but also security measures in other locations, are being discussed. How much do you agree or disagree with the following statements about some of these measures? 2. Governments should increase security checks in public places such as parks, shopping centres and other places where large groups gather.[279]

As with the previous question, in all countries surveyed there seems to be greater support in relation to agreeing to increase security checks in public spaces:

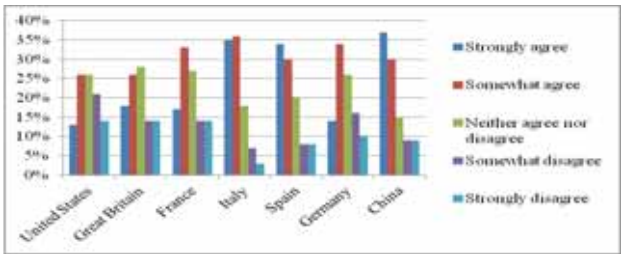


Figure 30: Financial Times/Harris Poll: Body scanners - public spaces and security checks[280]

[276] Ibid., p. 2.
[277] Ibid.
[278] Ibid.
[279] Ibid.
[280] Ibid.

As with the previous question, there are once again noticeable differences in responses between different countries. Those residing in China (37%) and Italy (35%) and Spain (34%) were more likely to "strongly agree" with the statement. In contrast those in the United States (21%), Germany (16%) and France (15%) were more likely to be those that would "somewhat disagree". There were a substantial percentage of individual's from Great Britain (28%), France (27%), the United States (26%) and Germany (26%) who neither agreed nor disagreed with the notion of increased security checks in public spaces to enhance security.[281]

The final question relevant to our analysis of public opinion regarding the trade-off between surveillance and security asks participants whether they think there is too much surveillance of individuals by governments. Researchers used the following question:

> Following the failed attempt to explode a bomb on a plane in America on Christmas day, certain measures to increase not only airline security, but also security measures in other locations, are being discussed. How much do you agree or disagree with the following statements about some of these measures?' 3. There is already too much surveillance of individuals by the government.[282]

The report revealed that responses to this question were somewhat mixed across all countries, with participants being more likely to select "neither agree nor disagree" than any other option:

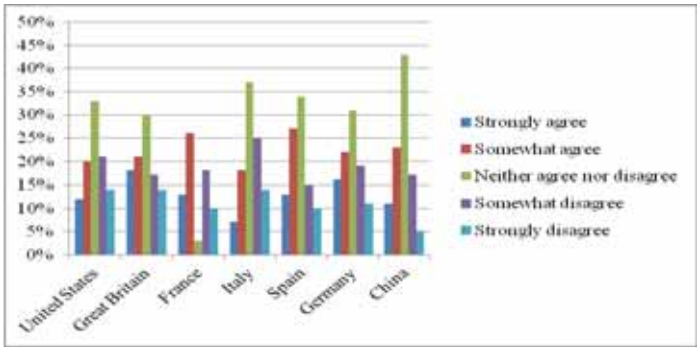


Figure 31: Financial Times/Harris Poll: Body scanners - government and surveillance – "there is already too much surveillance of individuals by the government"[283]

For those that did "strongly disagree", researchers found that responses were higher in Great Britain (18%) and Germany (16%). For those that selected "strongly disagree", responses were highest in the United States (14%), Great Britain (14%) and Italy (14%), those in China (5%) were least likely to "strongly disagree".[284]

4.14.3 *Relationship with other surveys*

In comparison to the 2002 Harris Poll which sought to understand the trade-off between surveillance and security, results from the present survey support previous findings that within the United States there is continual agreement with increasing surveillance to enhance security. The survey also identified similar attitudes to the *Flash Eurobarometer #225* in citizens' willingness to support greater surveillance measures to enhance security. However,

[281] Ibid.
[282] Ibid., p. 3.
[283] Ibid.
[284] Ibid.

this support is complex. Similar to the use of DNA surveillance above, measures focused on the body, such as body scanners, generate a fair amount of opposition. As illustrated in the survey, there has been a gradual decline in support for surveillance as a result of the impact it has on individuals' sense of privacy. A Washington Post/ABC Poll in 2006 also found that nearly two in three Americans surveyed said they believed that federal agencies involved in anti-terrorism activities are intruding on the personal privacy of their fellow citizens, but less than a third said such intrusions are unjustified. Thus people seem to accept that surveillance in necessary to enhance security, but their concerns surrounding the impact of privacy are growing.[285]

4.14.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers on the survey results. However, it is possible that some reports appeared in print form only, or in other languages. The survey has received attention in the news. For instance, Reuters released a press release of the survey's results.[286] Elsewhere, Just Luxe released a business wire highlighted news of the survey, focusing on confirming results concerning public acceptance of full body scanners in airports to increase security.[287]

This public opinion poll by Harris Interactive demonstrates that a complex and contradictory picture of individuals' support greater surveillance to help enhance security in airports. Those in some countries, notably Italy, are more supportive of increasing surveillance measures to enhance security. In contrast, those in Germany are more likely to disapprove of increasing surveillance measures to enhance security. Furthermore, respondents in multiple countries report being undecided over whether surveillance measures should be enhanced to improve security.

4.15 UNISYS SECURITY INDEX: GLOBAL SUMMARY

The *Unisys Security Index* is a regular survey conducted twice every year, the specific survey discussed here was published in April 2010.[288] Every six months, the survey provides insight into the attitudes of consumers in ten countries in relation to four security issues: national security, financial security, Internet security and personal security. Although this survey has revealed that financial threats are the greatest concern, this analysis will focus on the other three topics; national, Internet and personal security. However, financial security will be discussed in relation to its relationship with other categories, such as Internet security. The survey also provides us with some indication of public attitudes towards a trade-off between privacy and security / surveillance technologies.

---

[285] Balz, Dan, and Claudia Deane, "Differing Views on Terrorism", *The Washington Post*, 11 January 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/01/10/AR2006011001192.html

[286] "Most Adults in Largest European Countries, U.S. and China Agree Full Body Scanners Should Be Introduced in Airports", *Reuters*, 3 March 2010. http://www.reuters.com/article/2010/03/03/idUS94073+03-Mar-2010+BW20100303

[287] "Most Adults in Largest European Countries, U.S. and China Agree Full Body Scanners Should Be Introduced in Airports", *Just Luxe*, 3 March 2010. http://www.justluxe.com/syndicated-news/cid395272/Samenvatting-YOTEL--de-iPOD-uit-de-hotelbusiness-brengt-betaalbare-luxe-naar-New-York

[288] *UNISYS Security Index: Global Summary*, Lieberman Research Group, 13 April 2012. http://www.unisyssecurityindex.com/usi/global/reports

4.15.1 *Methodology*

The April 2010, *Unisys Security Index* survey was administered in February 2010 in three different ways: telephone, online and face-to-face. The survey gained a representative sample of adults over the age of 18 in 10 countries. Where necessary, researchers weighted the data they had collected with regard to national demographic characteristics.[289] The following table provides further details of the nature of the sample:

Table 9: Unisys security index - sample[290]

Country	Sample size	Administration method
Australia	1200	Telephone
Belgium	755	Face-to-face
Brazil	1500	Telephone
Germany	960	Telephone
Mexico	1031	Telephone
Netherlands	500	Online
New Zealand	532	Telephone
Spain	970	Face-to-face
UK	977	Telephone
US	1004	Telephone

Unisys expresses the results of their survey via a security Index that "runs from 0 to 300, where 0 represents no concern and 300 represent extreme concern". The following figure provides further information about this Index:

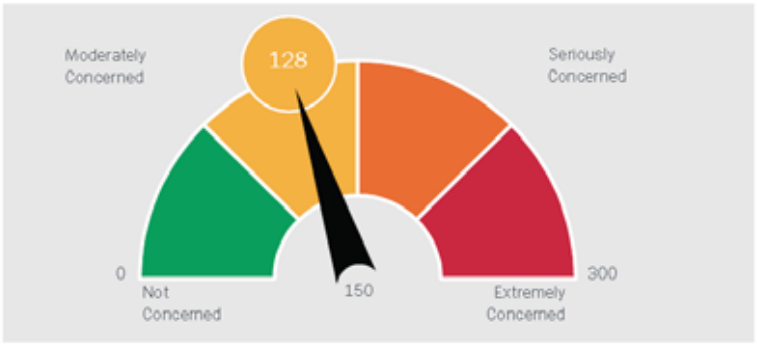


Figure 32: April 2010, Unisys Security Index[291]

4.15.2 *Main findings*

Across all four categories of security (national, financial, Internet and personal), concerns were highest in Brazil, Mexico, Germany and the US. Concern was lowest in the Netherlands and Belgium.[292] Findings suggest that adults are moderately concerned about financial security and least concerned over Internet security: 137 indices vs. 114 (across all 10 countries).[293] Although the questions are not included in the report, Unisys provide their

[289] Ibid., p. 4.
[290] Ibid., pp. 2 and 4.
[291] Ibid., p. 3. (*Note: This figure has been copied and inserted here from the report).*
[292] Ibid., p. 4.
[293] Ibid., p. 6.

readers with an indication of how the questions were derived. For instance, financial security is discussed in relation to:

> Other people obtaining and using your credit or debit card detail. Your ability to meet your essential financial obligations, such as your mortgage, other loan, credit card or bill payments.[294]

However, security issues may overlap. For instance, with regard to financial security (as identified above), the survey recognises that use of credit card could have occurred on the Internet:

> Computer security in relation to viruses or unsolicited emails. The security of shopping or banking online.[295]

However, the survey did not develop a wider understanding of the relationship between financial and Internet security, which could be the result of the limitations in the survey questions.

In this survey, the report states that national security was framed in relation to:

> National security in your country (for the US, UK, Australia and New Zealand, the question reads, "National security in relation to war or terrorism"). A serious health epidemic occurring in your country.[296]

Unisys did not provide any indication as to why some countries were singled out as being asked about war or terrorism. This is a potential flaw of the survey as Unisys did not ask participants about the same situation. Unisys considered serious concern over national security as a value of 150 or more. Countries that scored in this region included: Mexico (190), Brazil (189) and the US (182).[297] Those with moderate levels of concern included: Germany (149), the UK (151), Australia (132), Spain (125) and New Zealand (99). Those with lower levels of concern include Belgium (78) and the Netherlands (74).[298] In comparing these results to previous surveys, Unisys found that concern was lower in all countries with the exception of Brazil, UK and New Zealand.[299] Overall, the report revealed that respondents did not view national security as big a concern as personal security, but respondents did view national security as being more important than Internet security.[300]

Unisys measured personal security in relation to:

> Unauthorized access to or misuse of your personal information. Your overall personal safety over the next six months.[301]

Countries which indicated a serious concern over the threat of personal security report being more concerned about ID theft than personal safety; Mexico (192 vs. 190), Brazil (192 vs.

[294] Ibid., p. 5.
[295] Ibid.
[296] Ibid., p.5.
[297] Ibid., p.16.
[298] Ibid., p. 17.
[299] Ibid., p.15.
[300] Ibid., p. 6.
[301] Ibid., p. 5.

171), Germany (218 vs. 101). Those who felt that personal security was a moderate concern also indicated that they were more worried about ID theft than personal safety; examples include: US (177 vs. 109), Australian (175 vs. 61), Belgium (107 vs. 59).With the exception of Spain, concern over personal security increased between 2009 and 2010.[302] The survey did not examine the possible relationship between ID fraud and the Internet. Concerns over ID theft show a degree of concern towards the relationship between privacy and security. However, this is potentially a result of the measure used to understand perceptions of Internet security, where emphasis is placed on the threat of viruses, unsolicited e-mails, and security of shopping and banking online.[303]

The final area of concern for the Unisys survey is Internet security. As previously indicated, this area of security appears to be the issue that individuals are least concerned about – even though this area of security is linked to two other issues: financial and personal security. To reiterate, Unisys measure Internet security concerns in relation to:

> Computer security in relation to viruses or unsolicited emails. The security of shopping or banking online.[304]

Unisys identified moderate concerns over Internet security in eight of the 10 countries, with the exception of the Netherlands and Germany. In the majority of the eight countries, with the exception of Australia and the UK, concern is greater in relation to the threat of viruses than e-commerce.[305] Two countries with opposing views of Internet security are Germany and Spain. Germany (161 viruses, 150 e-commerce) seems to be much more concerned over the threat of both viruses and e-commerce than those in Spain (66 viruses, 62 e-commerce). In most countries, with the exception of Australia and Spain, concern over Internet security has increased between 2010 and 2009.[306]

The survey also has a supplementary question which seeks to understand the trade-off between surveillance, privacy and security:

> Which of the Following Statements Describe your Willingness to Sacrifice Some Privacy for Enhanced Personal Security and Convenience When you Travel by Air?
> - Full electronic body scans at the airport
> - Identity checks using biometric data such as iris scans or fingerprints
> - Provide personal data in advance such as a driver's license or passport[307]

Results suggest that the majority of individuals are willing to be subjected to one or more of the screening methods mentioned; more than 85% of individuals indicated this from all countries except Mexico (75%); all participants in Australia agreed. These results suggest that in light of enhancing security people are willing to forego their privacy.

The survey has not included any questions that provide an indication of measures that individuals may be taking to enhance their security.

---

[302] Ibid., p. 18.
[303] Ibid., p. 5.
[304] Ibid.
[305] Ibid., p. 22.
[306] Ibid., p. 20.
[307] Ibid., p. 24.

4.15.3 *Relationship with other surveys*

This survey currently stands out in our analysis as a result of its attention to a range of security issues: national, financial, Internet and personal. This survey found similar results to the *Flash Eurobarometer 225: Citizens perceptions of data protection*, where individuals are willing to be subjected to surveillance measures in the trade-off to enhance their security. Results from this survey are also congruent with results from the *Financial Times/Harris Poll: Body Scanners*. Specifically, respondents reported "some" willingness to forgo privacy by being subjected to enhances surveillance measures when travelling by air.

4.15.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages.

This survey is somewhat limited in its questioning and analysis of concern over security issues. Findings suggest that concern is greater over the issue of financial security than national, personal and Internet security; this is not necessarily a surprising revelation in light of the global recession in 2010.

4.16 PEW INTERNET & AMERICAN LIFE PROJECT: REPUTATION MANAGEMENT AND SOCIAL MEDIA

Pew Internet & American Life Project: Reputation Management and Social Media[308], published in 2010, sought to understand how individuals are choosing to manage their online in identity. Building on their 2007 digital footprints report, included in this analysis, the present study aims to explore the growing impact of managing an online identity using social media and what this means for a person's privacy and surveillance in the digital age.

Whilst this survey reveals findings relating to Americans digital footprints, in relation to our work on PRISMS, this analysis focuses on the survey's intention to further understand the growing impact of social media on privacy, and, as a result, public attitudes towards privacy and surveillance on the Internet. The survey also contains a minor point relating to the issue of trust.

4.16.1 *Methodology*

The findings of this report by *PEW Internet & American Life* stem from findings of the daily tracking survey on Americans' use of the Internet. A daily tracking survey is a survey that is carried out on a daily basis to a sample of Internet users. From a sampling perspective, this involves:

> New sample was released daily and was kept in the field for at least five days. The sample was released in replicates, which are representative subsamples of the larger

[308] Madden and Smith, 2010.

population. This ensures that complete call procedures were followed for the entire sample.[309]

This survey was administered via telephone interviews conducted by Princeton Survey Research Associate International. Researchers collected data between 18 August and 14 September 2009, gaining a total sample of 2253 adults aged 18 and older Researched selected the sample using a combination of landline and mobile phone random digit dial strategies.[310] Princeton Survey Research Associate International consider the sample to be a representative sample of American adults.

4.16.2 *Main findings*

As found in this survey, an individual's digital footprint has expanded over time. This could result in increasing levels of concern regarding the amount of personal information about individuals now available on the Internet. However, contrary to this perspective, findings from this PEW survey suggest that Internet users have become less likely to express concern about the size of the digital footprint. Between December 2006 and the present study there has been a 7% decline in the level of concern shown by individuals about their digital footprint (40% to 33%).[311] Those between the age of 30 and 49 are more likely to worry about the amount of information about them that is available online (38%); concern is lower among those aged between 18 to 29 (30%), those aged between 50-64 (31%) and those over the age of 65 (23%).[312]

The survey revealed that some people are taking measures to limit the amount of personal information about them online. For instance, findings from the survey suggest that 65% of social networking site users have changed privacy settings for their profile with the aim of enhancing or controlling their privacy online.[313] Researchers from this survey highlighted results that suggested that just because individuals were choosing to take measures to enhance their privacy that is not to say that they "worry" about their privacy:

> A relative lack of concern about the availability of personal information online does not necessarily translate into inaction. Indeed, many of the least concerned internet users have still taken steps to restrict what they share with others. For example, two-thirds of all SNS users (65%) say they have changed the privacy settings for their profile to limit what they share with others online. Among SNS users who worry about the availability of their online information, fully 77% have changed their privacy settings. However, even those who don't worry about such information are relatively active in this regard - 59% of these less concerned SNS users have adjusted their privacy settings in this way. [314]

Since the 2006 survey, there has been a decline in the proportion of individuals taking measures to protect themselves online. Only 32% of Internet users now take measures to protect themselves (compared to 38% in 2006).[315] As per the findings in 2006, younger

[309] PEW Internet & American Life Project, "About This Report: Reputation Management and Social Media - Methodology", 26 May 2010. http://pewinternet.org/Reports/2010/Reputation-Management/Methodology/About.aspx
[310] Madden and Smith, 2010, p. 7.
[311] Ibid., p. 21.
[312] Ibid.
[313] Ibid.
[314] Ibid.
[315] Ibid., p. 22.

individuals seem to be the age group who consistently continue to take measures to protect their identity online. Whilst older groups are limiting the amount of information they put online about themselves, there has been a small decline in the number of older respondents that are doing so since 2006.[316] Those individuals that spend more time searching for information about themselves and others on the Internet appear to be the ones who are most engaged with limiting the amount of personal information online (46% of active searchers vs. 33% of non-active searchers).[317]

The survey has also revealed a correlation between having a bad experience regarding their personal information online and being concerned with taking measures to limit their information online. Those who have had a bad experience online appear to worry and then take measures to limit the amount of personal information available about them on the Internet (7% vs. 3% who do not worry).[318]

Results from the survey reveal important insights with regard to the extent to which adults trust Internet companies. Researchers used the following question: "How much of the time to you think you can trust the following?". Researchers are respondents about a series of "types" of organisations: large corporations, newspapers and television news, financial companies, news websites, social networking sites and websites that provide health information. Of the six categories, Internet users were more likely to distrust social networking sites (65%), and younger adults (those aged between 18 and 29) were most distrustful of social networking sites. The category that attracted the most trust from users was news websites. Those between the age of 18 and 29 were more likely to "always trust" news websites (11%). Those between the age of 30 and 49 were more likely to trust newspapers and television news (6%) and those aged over 50 were more likely to always trust websites that provided them with health information (6%).[319]

4.16.3 *Relationship with other surveys*

As with other surveys included in this analysis, such as the *Special Eurobarometer 359: Data protection and e-Identity,* this survey provides further evidence that individuals are concerned about the amount of personal information available about them on the Internet. As opposed to the *PEW Internet & American Life Project: Digital Footprints* (2006), this survey has revealed that there has been a decline in the number of individuals that expressed being concerned about their digital footprints. Furthermore, this survey has found that the number of people that are taking measures to enhance their security online has decreased.

4.16.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages.

Findings from this survey suggest adults in the United States are becoming less concerned about the amount of information available about them that is available online. The findings from this 2010 survey sit in contrast to the 2006 digital footprint survey on this issue. Despite

[316] Ibid.
[317] Ibid., p. 24.
[318] Ibid., p. 27.
[319] Ibid., p. 33.

these findings, some individuals continue to take measures to limit the amount of personal information available about them on the Internet. Findings from this latest survey have also revealed that users are becoming increasingly distrustful of social networking sites.

4.17 EU KIDS ONLINE: RISKS AND SAFETY ON THE INTERNET – THE PERSPECTIVE OF EUROPEAN CHILDREN

The *EU Kids Online survey*[320] was carried out in October 2010, as part of a work package for the European Commission's Safer Internet Programme. The survey was organised by the EU Kids Online consortium, which was co-ordinated by the London School of Economics (LSE). Guidance for the survey was given by Ipsos MORI, a global research company.[321] The aim of the survey was to develop a wider understanding of children's use and experiences of the Internet in the European Union, with supplementary information from parents. Results from the survey would then be used by the projects consortium to provide recommendations for "national and international stakeholders of a safer online environment for children".[322] The survey covers a range of topics, examples include: usage, online activities, networking and online risks.

The survey is relevant to our work on PRISMS as it provides us with information regarding privacy and security on the Internet from a sample of children, which is useful as the majority of surveys investigate adult attitudes rather than those of children.

4.17.1 *Methodology*

This survey was conducted between April and August 2010. The survey was aimed at 25 European Union Member States, and included a final sample of 23,420 children, aged 9 to 16.[323] For the majority of countries, approximately 1000 participants were involved (with the exception of: Cyprus, Ireland, Norway, Slovenia and Sweden – where numbers were lower).[324] Researchers selected the sample using a stratified sample, by region and level or urbanisation. The survey was administered by researchers via face-to-face interviews, aimed at both children (9 to 16 years of age) and their parents. For sensitive questions, researchers gave participants a self-completion questionnaire. Within an individual's home, where there was more than one child, researchers took a random sample of a single child was taken; researchers selected parents based on who knew more about the child's Internet usage.[325]

4.17.2 *Main findings*

The use of the Internet by children is important to our contextual understanding of children's safety and attitudes to accessing and interacting with others on the Internet. Results from this survey suggest that young people's use of the Internet across Europe is widespread. Access begins from a young age but varies across different age groups, suggesting that users are access the Internet at a younger age as time passes. For instance, the average age of 9-16 year

[320] Livingstone, Sonia, Leslie Haddon, Anke Gorzig and Kjartan Olafsson, *Risks and Safety on the Internet: The Perspective of European Children: Initial Findings*, London School of Economics, 2010. http://www.ipsos-mori.com/researchpublications/publications/publication.aspx?oItemId=1392
[321] Ibid., p. 120.
[322] Ibid., p. 2.
[323] Ibid., p. 11.
[324] Full details on the sample size can be found in the report (Ibid., p. 122).
[325] Ibid., p. 120.

olds first use of the Internet is 9 years of age, whilst those aged between 15 and16 were 11 years old when they first went online.[326] In terms of use, the survey also found that children were accessing the Internet more often than their parents.[327] The average time spent on the Internet by those ages between 9 and 16 is approximately 86 minutes per day.[328] In relation to PRISMS, the fact that children are using the Internet at such a young age, and so frequently, makes them a relevant sample of the population to take into consideration.

The activities that children are taking part in online are also of interest as this provides further contextual information as to how behaviour can influence perceptions of privacy and security on the Internet. The nature of children's activities is widespread; children are involved in a range of activities that involve divulging personal information and interacting with others. For instance, in the last month 61% of the sample claimed they used the Internet for instant messaging; 60% visit asocial networking website, 44% played games with other people online, 38% shared photo's or video's with others and 22% visited a chatroom.[329]

Across Europe, 57% of the sample reported having their own profile on a social network. These findings vary across gender and age; slightly more girls than boys have their own profile (58% vs. 56%). In relation to age, 15-16 year olds are more likely to have a profile than other age groups; the following figure provides further information:

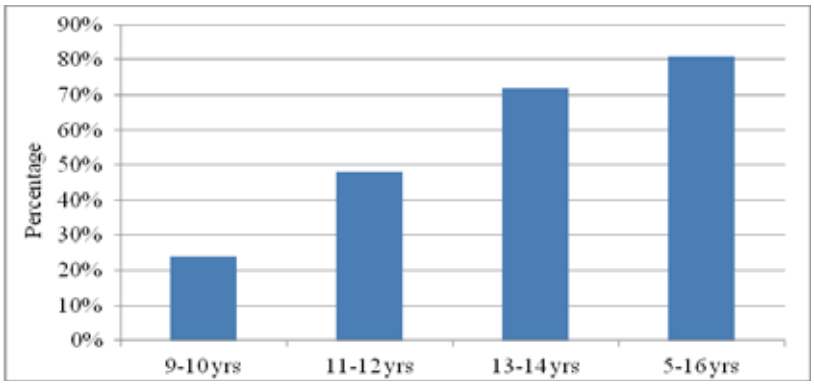


Figure 33: EU Kids Online - age and use of social network sites[330]

When breaking results down by country, researchers identified noticeable differences across European Union Member States. Those in the Netherlands, Slovenia and Lithuania (78%, 76% and 75% respectively) are more likely to have a profile on a social networking site than those in Germany, Turkey, and Romania (50%, 47% and 47% respectively).[331]

The survey revealed important findings regarding the relationship between use of social networking sites and privacy settings. Researchers provided participants with four options to choose from concerning how they set their privacy settings: private, partially private, public, don't know.[332] Responses varied in terms of both gender and age. Girls were more likely than boys to indicate that they kept their profile private (45% vs. 36%). Both genders were equally

[326] Ibid., p. 27.
[327] Ibid., p. 36.
[328] Ibid., p 30.
[329] Ibid., p. 38.
[330] Ibid., p. 40.
[331] Ibid., p. 41.
[332] Ibid., p. 42.

likely to indicate that their profiles were partially private (28%). Boys were more likely than girls to state that their profile was public (33% vs. 24%). Those aged between 11 and 12 years were more likely to have a private profile than other age groups. The oldest (15-16 years) and youngest group (9 – 10 years) were more likely to answer that their profile was public than the other groups.[333] There is, therefore, some evidence to suggest that some children are aware of the importance of privacy in relation to social networking sites, and are accordingly, taking measures (in the form of privacy settings) to enhance their privacy.

The survey revealed further insights regarding privacy and security when researchers asked respondents about whether they had experienced any trouble with the misuse of their data on the Internet:

> In the PAST 12 MONTHS, has any of the following happened to you on the internet?
> Somebody used my password to access my information or to pretend to be me.
> Somebody used by personal information in a way I didn't like
> I lost money by being cheated on the Internet.[334]

Results suggest that very few children had experienced misuse of their data as asked in this survey; only 9% of the sample responded that they had experience one or more of the statements presented to them. The most common misuse appeared to be in relation to the first statement, that somebody had used their password to access their information or pretended to be them (7%). This was followed by someone misusing their personal information (option 2 above) (5%). Only 2% reported having their data misused in relation to losing money.[335]

In relation to the issue of security, due to the sensitive nature of the line of questioning, the survey included two questions for respondents to answer:

> Do you think there are things on the internet that people about your age will be bothered by in any way? In the past 12 months, have you seen or experienced something on the internet that has bothered you in some way?[336]

The concept of security appears to have been operationalised by asking individuals if they had been "bothered" by something they had experienced. The first line of questioning, asks respondents about their perceptions, while the second line of question asks them about the behaviour. By combining the two, researchers are able to further understand the relationship between perceived and actual security on the Internet. Results suggest that within all age groups more than 50% of children believed that there were things on the Internet that were capable of "bothering" other children their age. In comparison, very few had actually experienced being bothered by something online; showing a discrepancy between the two.[337] In addition to asking this question to children, researchers asked their parents whether their children had been exposed to anything on the Internet that had bothered them in some way. In all age groups, parents seemed to be less aware that their children had experienced something on the Internet that bothered them, which shows a difference between what children had experienced and what their parents knew of their child's online experiences.[338]

---

[333] Ibid.
[334] Ibid., p. 103.
[335] Ibid.
[336] Ibid., p. 50.
[337] Ibid.
[338] Ibid.

Other areas of security concerns discussed in the survey were related to exposure to sexual content, harmful user-generated content and bullying on the web. Results from the survey show that within all age groups, some children (14%) have been exposed to sexual images on the Internet. When comparing this to parents' perceptions, as with the previous line of enquiry, parents are not entirely aware of what their children are exposed to (12% compared to 14%).[339] In terms of whether this exposure is a harmful to children, from a child's perspective, one in three European children claimed they had been bothered by what they saw.[340] When asked how the child had coped with what they had seen, results show that some are taking measures to prevent this from happening again. For instance, 21% claimed that they were trying to fix the problem (compared to 25% who hoped the problem would go away by itself, 11% felt guilty and 44% did respond in any of the ways mentioned). Individuals used a variety of strategies to respond to the situation they had faced, this ranged from telling someone to more proactive responses such as using specific tools to prevent future occurrences, examples include: deleting messages received (29%), blocking the person who had sent them something (22%); stopping using the Internet for a while (24%); reporting the problem with a "report abuse" button (13%), don't know (29%). Thus, some children took various steps to help ensure their safety, but others simply did not know what options were available (29%).[341]

Second, the survey allows a consideration of the issue of bullying online. The survey designers defined bullying as follows:

> Sometimes children or teenagers say or do hurtful or nasty things to someone and this can often be quite a few times on different days over a period of time, for example. This can include: teasing someone in a way this person does not like; hitting, kicking or pushing someone around; leaving someone out of things.[342]

Following this definition, researchers informed respondents that this form of bullying could take place via three forms: in person, via a mobile phone or on the Internet. The survey then asked children whether they had personally experienced any of these forms of behaviour in the last 12 months. Results suggested that within Europe, 19% of 9-16 years old had been faced with this form of behaviour, with very little demographic-based differences.[343] When faced with different types of bullying, children were more likely to have experienced face-to-face bullying than that via the Internet or a mobile phone.[344] When asked how the child responded to the situation of being bullied on the Internet, responses were more likely to be either "proactive", in the sense that they took action against it (39%) or "fatalistic", in that they would hope that it would stop (21%).[345] For those who were "proactive", as with responding to being confronted with sexual images, measures taken ranged from: "I stopped using the internet for a while" (21%), "I deleted any messages from the person who sent it to me" (45%), "I changed my filter/contact settings" (18%), "I blocked the person who had sent it to me" (41%), "I reported the problem (e.g., clicked on a 'report abuse' button, contact an internet advisor or internet service provider (ISP)" (12%), "none of these" (8%), "don't

[339] Ibid., p. 57.
[340] Ibid., p. 60.
[341] Ibid., p. 64.
[342] Ibid., p.67.
[343] Ibid.
[344] Ibid., p. 68.
[345] Ibid., p. 76.

know" (18%).[346] Thus, many children strive to take action to help improve their situation, and in this case, their sense of security.

When comparing results across European Union Member States, those living in a country with greater daily Internet use were more likely to report being at risk. Countries aligned to this include: Czech Republic, Estonia, Finland, Bulgaria, Belgium, Poland and Romania. Countries whose children were less likely to access the Internet on a daily basis and therefore not be in as much risk included: Hungary, Spain, Italy, Portugal, Greece, Ireland and Turkey.[347]

4.17.3 *Relationship with other surveys*

This survey has highlighted, along with the *Online Profile & Reputation Perceptions Study* (see section 2.19.2) that young people are concerned with their privacy on the Internet. The survey identified similar findings with regard to adults and children taking action to enhance privacy online; some try to enhance their security and privacy on the Internet, others however, simply do not necessarily have the knowledge to use the necessary tools. In contrast to other surveys, this question raises the issue of security in relation to being "bothered" by something or bullied; this is not something that is addressed in other surveys, and is not necessarily restricted to young people, forcing us to further consider how we come to understand the issue of "security" on the Internet.

4.17.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages. News of the survey was, however, released via a series of websites ranging from news of the survey by the UK's children's charity, Save the Children[348], as well as websites designed to help parents support their children in the digital world; Kids and Media[349]. In both instances, the websites publicised news of the survey, and the parental guidance website also included recommendations given in the report.

EU Kids Online distinguishes itself from other surveys in its attempt to survey young people's experiences of life on the Internet. In relation to our work on PRISMS, this survey demonstrates that alongside adults, some children are taking measures to enhance their privacy, security and sense of safety on the Internet. However, this ability to take responsibility for personal safety on the web is largely affected by knowledge, awareness and understanding of tools to enhance both privacy and security.

---

[346] Ibid., p. 77.
[347] Ibid., p. 112.
[348] Save the Children: Resource Center on Child Protection and Child Rights Governance, "EU Kids Online - Towards a Better Internet for Children", 2012.
http://resourcecentre.savethechildren.se/content/library/documents/eu-kids-online-towards-better-internet-children
[349] Rasmussen, Rune, H., and Sigrun Landro Thomassen, "EU Kids Online: New Approach to Online Safety Required", Kids and Media, 25 October 2011. http://kidsandmedia.org/eu-kids-online-new-approach-to-online-safety-required/

4.18 SPECIAL EUROBAROMETER 359: ATTITUDES ON DATA PROTECTION AND ELECTRONIC IDENTITY IN THE EUROPEAN UNION

Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union[350] was published in June 2011. As suggested by the title, the aim of this European survey was to develop a wider understanding of public opinion relating to the disclosure of personal information as well as attitudes relating to privacy, security and trust of personal data. The survey was carried out on behalf of the European Commission and was the result of co-operation between a series of groups: "TNS opinion and the eID team at the Institute for Prospective Technological Studies (IPTS) of the Joint Research Centre (JRC) in cooperation with DG JUST."[351]

Whilst this survey provides a comprehensive amount of information regarding what individuals are disclosing and how they think data should be regulated, this Special Eurobarometer is particularly relevant to PRISMS as it focuses on exploring all four of our areas of interest: public perceptions of disclosure in relation to their privacy, surveillance in society, security online and the issue of trust in relation to organisations handling of personal data. Importantly, this survey also offers the opportunity to engage with an up-to-date understanding of the various measures European citizens may be taking to enhance their security on the web.

4.18.1 *Methodology*

The survey was conducted between the 25 November and the 17 December 2010; results were published in June 2011.[352] The survey, carried out by TNS Opinion and Social used face-to-face surveys, which took place in participants' homes in the appropriate language. The survey consisted of a representative sample of 26574 individuals (over the age of 15) from 27 European Union Member States.[353] TNS selected the sample using a multi-stage random sampling strategy.[354] Full details regarding sample figures can be found in the annex (Annex 1) of the report.

4.18.2 *Main findings*

This survey used "disclosure of personal information" as a conceptual tool for understanding public attitudes relating to the sharing of personal information and what this means for individuals privacy. Many respondents (74%) viewed disclosure of personal information as being part of everyday life.[355] Responses ranged across different countries; those in Denmark, Greece and Sweden were more likely to agree with this argument than those in countries such as Romania, Hungary and Malta.[356] From a socio-demographic perspective, the younger the individual the more they were likely to agree with the statement. In addition, more educated individuals were also likely to agree. Everyday Internet users were also more likely to feel

[350] TNS Opinion and Social, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, Special Eurobarometer, European Commission, 2011. http://ec.europa.eu/public_opinion/archives/eb_special_359_340_en.htm
[351] Ibid., p. 9.
[352] Ibid., Annex.: Technical Specification (no page number included).
[353] Ibid., p. 9.
[354] Ibid., Annex.: Technical Specification (no page number included).
[355] Ibid., p. 22.
[356] Ibid., p. 23.

that disclosure of personal information was an increasing part of everyday life.[357] Unfortunately, the report did not include any information to show whether there were any gender differences in the answering of this question.

When asked whether disclosing personal information was a big issue for them, the majority, 63%, felt it was, while 33% of respondents said it was not.[358] Responses differed according to country. For instance, those in Denmark (51%), Estonia (47%) and Lithuania (46%), were more likely to think that disclosing personal information was not a "big deal". Alternatively, those in Greece (75%), France (74%), and Malta (71%) were more likely to feel it was a "big deal" to disclose personal information.[359] From a socio-demographic perspective, younger participants (those aged between 15 and 24) and those who were still studying were more likely to agree that it was not a big issue.[360] Researchers identified small differences in perceptions in relation to gender, where men were more likely than women to "agree" that disclosing personal information was not a big issue for them (36% vs. 31%). Conversely, both men and women were more likely to indicate that disclosing personal information was a big issue for them (60% and 64% respectively).[361] Additionally, those individuals that were more likely to be part of a social networking site and those who shared pictures, videos, and movies were also more likely to believe that it was not a problem.[362] These results suggest that whilst disclosing personal information may be part of everyday life, but that is not to say that people are not concerned by it.

In an attempt to further understand concern over the disclosure of personal information, the survey then went on to directly ask respondents how concerned they were about "over disclosure". Here "concern" is used to measure attitudes in relation to worry and anxiety over disclosing information.

Table 10: Concern about over-disclosure[363]

Concern	Percentage
Very concerned	19%
Fairly concerned	53%
Not very concerned	24%
Not at all concerned	3%
Don't know	1%

Results from the survey suggest that the majority (53%) of respondents were fairly concerned, only 3% were not concerned at all.[364] The level of concern a person held was attributed to where they were from. Those who were not concerned with the unnecessary disclosure of personal information were more likely to come from Sweden (66%), the Netherlands (51%) and Malta (49%). Those who were concerned were more likely to come from Lithuania (83%), Ireland (82%), Portugal (82%) and Greece (82%).[365] From a socio-demographic

[357] Ibid., p. 24.
[358] Ibid., p. 22.
[359] Ibid., p. 30.
[360] Ibid., p. 31.
[361] Ibid.
[362] Ibid., p. 32.
[363] Ibid., p. 54.
[364] Ibid.
[365] Ibid., p. 55.

perspective, those who indicated that they were not concerned were more likely to be 15-24 year old students. Concern was rated higher by older respondents (40-54 and older than 55 years).[366] In relation to Internet use; the higher the Internet use, the lower the level of concern.[367] A broader understanding of the relationship between concern and education and gender was not provided.

Researchers then asked respondents what they were concerned about, allowing researchers to establish what risks people were worried about. The question used in the survey was:

> I will read out a list of potential risks. According to you, what are the most important risks connected with disclosure of personal information…[368]

Of those mentioned, in relation to their use of social networking sites, respondents were most concerned about their information being used without their knowledge (44%), followed by being a victim of fraud (41%), and information being shared with third parties without their knowledge (38%). Respondents were least concerned about being discriminated against (e.g., in relation to job selection) (7%), their views being misunderstood (11%) and their reputation being damaged (12%). Respondents were also concerned about the risks of disclosure of personal information in relation to the purchasing of goods and services on the Internet: respondents were most concerned about being a victim of fraud (55%), followed by their information being used without their knowledge (43%). Respondents were least concerned about being discriminated against (e.g., in relation to job selection) (3%), their views being misunderstood (4%) and their reputation being damaged (4%). When asked about personal security in relation to both categories, only 20% of those using social networking sites considered this a risk, and 12% of those who disclosed their information in the purchasing of goods and services.[369]

An analysis of the socio-demographics of these results regarding risks and disclosure of personal information indicate some important issues. For example, in relation to the disclosure of personal information on social networking sites and potential risks involved, the older the individual, they were slightly more likely to feel that their information could be used without their knowledge (55 years old and above – 46%; 15 to 24 years – 43%).[370] Researchers did not find any differences in relation to gender and the risk of information being used without a person's knowledge.[371] The survey did, however, identify differences with regard to education and concern over information being used without a person's knowledge; the longer a person stayed in education the more they were likely to be concerned.[372] Alternatively when considering age and the risk of being a victim of fraud during the purchasing of goods and services, the survey revealed that younger individuals reported a slightly greater concern (15-24 years old- 57%; 55 and above – 52%).[373] The survey found barely any difference between the reported risk of being a victim of fraud and gender and education.[374] These findings are important to understanding how a person's socio-demographic background can influence citizens risk perceptions, which may then be used to

[366] Ibid.
[367] Ibid.
[368] Ibid., p. 57.
[369] Ibid.
[370] Ibid., p. 62.
[371] Ibid.
[372] Ibid.
[373] Ibid., p. 63.
[374] Ibid., p. 62.

tackle and help improve confidence as they enable policy makers to understand what about a person's background might influence their sense of security on the Internet.

Researchers asked respondents more generally about their concern about their behaviour being recorded in everyday settings as well as on the Internet. Within this survey, researchers operationalised the concept of surveillance via the term "recording":

> Nowadays, cameras, cards and websites record your behaviour, for a range of reasons. Are you very concerned, fairly concerned, not very concerned or not at all concerned about your behaviour…?[375]

Across the sample, respondents were more likely to indicate that they were "concerned" about their behaviour being recorded via payment cards – location and spending (54%) and mobile phone/Internet monitoring – call content and geo-location (49%). Participants were "not concerned" about being recorded in a public space (62%).[376]

The survey also offered an insight into what measures European citizens take to help protect their identity. Researchers used the following question:

> In your daily life, what do you do to protect your identity? Please indicate all that apply in the following list.[377]

The most common measure taken is to provide the minimum required information (62%), followed by avoiding disclosing bank details or their pin number (56%). Additional measures included avoiding sharing personal information with people or organisations they did not trust (47%) as well as avoiding sharing their user name and password (45%). Fewer respondents stated that they would not disclose payment details online (29%), shred private information, such as bills (29%), or provide inaccurate information (7%).[378] Thus it appears that there are limitations to what people will do to protect their identity; reasons for this behaviour were not explored in the survey, nor were they provided. When comparing results by country, the Netherlands and the Scandinavian countries were more likely to have taken certain measures to protect their identities. They were also the countries that were less concerned about their behaviour being recorded; perhaps a result of their actions to protect their identity. Measures were less likely to be taken in Southern European, Baltic and central countries; Poland, Hungary and Romania.[379]

Measures taken ranged according to age and type of measure. For instance, older individuals (over the age of 55) were more likely to shred documents with personal data than those aged between 15 and 24 (33% vs. 17%).[380] Across all categories of types of measures, those who had been in education over the age of 20 were more likely to have taken measures to protect their identity than those who had stayed in education until they were 15.[381] The survey revealed that education played a role in influencing the type of measures people may take. In general, the longer an individual spend in full-time education, the more likely they were to

[375] Ibid., p.64.
[376] Ibid.
[377] Ibid., p.100.
[378] Ibid.
[379] Ibid., p.102.
[380] Ibid., p. 105.
[381] Ibid.

have taken all measures asked about.[382] Unfortunately, researchers did not provide a gendered analysis in the presentation of results.

When asked what measures individuals take to protect their identity on the Internet, 15% stated that they did not take any measures.[383] Elsewhere, evidence suggests that some individuals would take measures online to protect their identity. Examples include (but are not limited to): protecting themselves against spam e-mail (42%), checking the security of the site they are using for a logo during a transaction (40%), use anti-spyware (39%) and delete cookies (35%). Respondents were less likely to take steps that involved them taking some form of "individual initiative" to protect their identity such as asking website for access to your data to remove it (8%), or use a dummy e-mail account (12%).[384] As with the previous question, those in Denmark and other Scandinavian countries were more likely to take measures to help protect their identity online, adoption was least likely in Baltic countries and Eastern European Member States.[385] From a socio-demographic perspective, education seems to have made the greatest difference: the longer an individual stayed in education, the more likely they were to have taken measures to protect their identity online.[386] Men were found to be more likely than women to have taken measures to protect their identity.[387] Once again, researchers did not query respondents with explanations or rationales to provide them with further information about this decision making process.

The survey included a question in relation to behaviour and privacy protection, where researchers asked respondents whether they read privacy statements online before providing their consent:

> Thinking about privacy statements on the Internet, which of the following sentences best describes your situation?[388]

The majority of participants stated that they read privacy statements (58%). A further 25% stated that they "usually do not" read them, 5% stated that they did not know where to find them, 8% stated that they ignored them and 4% stated they did not know.[389] Researchers did not identify any significant differences for ignoring privacy statements across different socio-demographic variables.[390] Those who indicated they did usually read them were more likely to be male (37%) as opposed to female (31%). They were also more likely to be aged 25-39 (38%), had been in school past the age of 20 (39%) and were likely to be daily Internet users (37%).[391] The most common reason cited for not reading privacy statements included: "it is sufficient for you to see that websites have a privacy policy" (41%). Other responses included believing the law would protect them (27%), thinking the website would not honour their privacy policies anyway (24%) and stating "I don't know" (15%).[392]

---

[382] Ibid.
[383] Ibid., p. 106.
[384] Ibid., p. 107.
[385] Ibid., p.108.
[386] Ibid., p. 111.
[387] Ibid.
[388] Ibid., p. 112.
[389] Ibid.
[390] Ibid., p. 114.
[391] Ibid.
[392] Ibid., p. 118.

The majority of those who stated that they read privacy statements indicated that they had changed their behaviour as a result (70%).[393] However, the survey did not include any additional questions that could have examined why or how they had changed their behaviour.

In addition to being asked about their attitudes and actions regarding the privacy of data online, researchers also asked individuals about security threats relating to identify theft and data loss that they or a relation had experienced online:

> In the last 12 months, have you heard about or experienced issues in relation to data losses and identity theft?[394]

Only 2% of those sampled had personally encountered a security breach in relation to identity theft. Forty-four per cent had not heard of anyone else having this experience. Those who had heard were more likely to have heard about identity theft via the news or Internet (42%), word of mouth (13%), an acquaintances experience (7%), or the experience of a member of their family (3%).[395] Thus, personal experience with identity theft was extremely low across the EU. Being personally affected occurred more often in the UK and Sweden (both 5%). Those in Latvia (69%), Sweden (62%), and Denmark (61%) were most likely to have heard about identify theft via the news or Internet.[396] From a socio-demographic perspective, personal experience of identity theft occurred more often in those aged between (25 and 54) (3% each), those who had been in education for 20+ years (3%). The survey found very little evidence of any relationship between the amount of time spent on the Internet and respondents reporting that they had personally experienced identity theft (1%). Similarly, the survey found very little evidence of any correlation between gender and whether an individual had personally experience identity theft (1%).[397]

The final area of consideration for our work on PRISMS relates to the extent to which individuals trust institutions and companies with their personal data. The survey included the following question:

> Different authorities (government departments, local authorities, agencies) and private companies collect and store personal information. To what extent do you trust the following institutions to protect your personal information?[398]

Individuals were more likely to trust institutions such as health and medical care (78%) and national public authorities (70%) than shops (39%), communication companies (32%), and Internet companies (22%).[399] As identified within the survey: "a majority of Europeans were concerned about their behaviour being recorded via payment cards, their mobile phone or on the Internet. That concern might be related to the limited trust in commercial organisations that collect these data."[400]

The survey reveals a relationship between different countries and trust; those in Denmark, Luxembourg, Finland and Sweden appear to be the most trusting. Alternatively, those in

[393] Ibid., p. 115.
[394] Ibid., p. 132.
[395] Ibid. Note: Respondents could select multiple answers.
[396] Ibid., p. 133.
[397] Ibid., p. 134.
[398] Ibid., p. 137.
[399] Ibid., p. 138.
[400] Ibid.

Romania and Greece are less trusting.[401] From a socio-demographic perspective, young people seem to be more trusting of public intuitions and commercial companies than older populations. Also, women are more likely to have trust in both public institutions than men. For instance, in relation to trusting health and medical institutions, 79% of women stated they trusted them as opposed to 77% of men. Conversely, men are more likely to have slightly more trust in commercial organisations than women. If we take the example of trust in Internet companies – 23% of men trusted them as opposed to 21% of women. In addition, the longer and individual stays in education the more trusting they seem to be. Lastly, greater use of the Internet appears to also make people more trusting.[402]

4.18.3 *Relationship with other surveys*

The survey's findings with regard to concern over geo-location and personal privacy has also been highlighted in a study from 2010 by *Webroot*; a company specialising in the protection of personal information on the Internet. The study of 1500 social network users found that although people were using geo-location ready mobile devices, 55% of the sample was worried about their loss of privacy.[403] Additionally, this survey has revealed similar results to the *Special Eurobarometer 359 "E-Communications Household Survey"* published in 2010, which found that a substantial number of individuals (84%) would want to know if their personal data had been lost, stolen or altered in any way.[404] The survey identified a significant increase from 2006, suggesting that individuals are becoming increasingly interested in the safety and protection of their personal data. In the US in 2008, the PEW Research Centre also found concerns over the sharing and selling of information as a result of online activities (in this case the use of cloud computing services).[405] Finally, findings from this survey also concur with other surveys examining issues relating to personal data. For example, the 2008 *Flash Eurobarometer #225* shows that individuals are more trusting of public institutions that commercial companies in being able to handle their personal data.

4.18.4 *Use of the survey results*

In January 2012, the European Commission used the results of the *Special Eurobarometer #359* to help rationalise the various reforms they propose to make to the 1995 Data Protection Directive. The Commission argued that existing rules from 1995 are in need of updating as a result of "rapid technological developments and globalisation".[406] For instance, the Commission cited Europeans' attitudes towards data protection (e.g., the lack of control people feel they have in relation to their data) as evidence to help support policy reform.

The *Special Eurobarometer #359* is an essential up-to-date survey to be included in our analysis of existing public opinion surveys in relation to security, privacy, surveillance and

---

[401] Ibid., p. 139.
[402] Ibid., p. 145.
[403] "Webroot Survey Finds Geolocation Apps Prevalent Amongst Mobile Device Users, But 55% Concerned About Loss of Privacy", *Webroot*, 13 July 2010. http://www.webroot.com/En_US/pr/threat-research/cons/social-networks-mobile-security-071310.html
[404] TNS Opinion and Social, *Special Eurobarometer 335: E-Communications Household Survey*, European Commission, October 2010, p. 157. http://ec.europa.eu/public_opinion/archives/ebs/ebs_335_en.pdf
[405] Horrigan, John B., *Use of Cloud Computing Applications and Services*, Data Memo, PEW Internet, PEW Internet & American Life Project, September 2008, p. 2.
http://www.pewinternet.org/~/media/Files/Reports/2008/PIP_Cloud.Memo.pdf
[406] European Commission, "Why Do We Need an EU Data Protection Reform?", 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT

trust in the digital era. The survey involved a representative sample of Europeans has demonstrated that many Europeans consider data sharing to be part of everyday life. Whilst many Europeans seem to accept this, they are concerned about the consequences of sharing their personal data and what this may mean for the security of their personal data and identity. The survey also includes evidence of differences in Europeans' trust towards different companies and their management of personal data. As a final point of consideration, this survey has shown that attitudes relating to this area of interest are dependent on a person's nationality as well as a variety of socio-demographic variables.

4.19 Online Profile & Reputation Perceptions Study

The *Online Profile and Reputation Perceptions Study* was conducted *Blueocean Market Intelligence*[407], written up by Brackenbury and Wong on behalf of the Microsoft Corporation[408] and published in 2011. The aim of the study was to understand public attitudes towards the creation and consequences of having an online profile. This survey is relevant to our work on PRISMS as it enables us to develop an insight into public perceptions relating to privacy and the security of individuals' personal profiles that they actively create and monitor on the Internet. The survey also provides us with an opportunity to understand the various measures that users may be choosing to take to enhance their privacy and security online.

4.19.1 *Methodology*

The research involved 5000 interviews with 1000 respondents from the US, Germany, Ireland, Spain and Canada.[409] Interviews took place between 11 and 24 November 2011. Respondents consisted of three age groups each of which had a different interview methodology. Young people between the ages of 15 and 17 and adults between the ages of 18 and 74 participated in direct interviews, while the parents of those aged between 8 and 14 reported indirectly on their child's activities.[410]

During the survey, researchers provided the respondents with examples of what types of material constitute to having an "online profile", and furthermore, how one could gain a "reputation" on the web:

> An online profile is created by one's interactions in the online world including the use of (Internet enabled) TV, mobile phones, Internet and worldwide web, gaming and other devices. Here are some examples:
>
> - Content about you (e.g., bank records, retail and airline purchases, telephone records, medical records, credit card purchases, etc.)
> - Content that you create online (e.g., email, text messages, images, audio, video, presence on social networks)
> - Your presence created by others (e.g., someone posting a picture or comments –about you on a social network or website, etc...)

[407] Ibid., p. 2.
[408] Brackenbury, Ian, and Thomas Wong, *Online Profile & Reputation Perceptions Study*, Microsoft Corporation, 2011. http://go.microsoft.com/?linkid=9797356
[409] Ibid.
[410] Ibid.

> Online reputation is the image created of you through information you or others shared online in blogs, posts, pictures, tweets, videos, etc.[411]

An "online profile" consists of those activities that individuals choose to participate in when using the Internet. An "online reputation" involves the identity and "image" that is developed about a person via the personal posting and sharing of personal information.

As will be seen in the subsequent section, all questions included in the interviews contain direct questions where elements such as "concern" and "control" are not defined; rather the designers of the survey appear to have assumed that respondents will understand their meaning.

4.19.2 *Main findings*

To begin with, results from the study enable an understanding as to what activities individuals think contributes to their online profiles:

> Q1. Of the online activities that you participate in, which three do you think contribute most to your own online profile?[412]

Responses to this question differed between adults and children; adults were more inclined to believe that their "e-mail" activities were more likely to contribute to their online profile (72%), compared to 48% of children.[413] Children were more likely to believe that their online profile was likely to be influenced by their activities on social networking websites than adults (42% vs. 31%). Adults also highlighted online shopping (32%) and online banking (31%) as contributing to their social networking profiles. Alternatively, for children, activities that they believed influenced their online profiles included: playing online games (42%) and downloading or streaming music, videos or movies (41%).[414] Adults and children therefore differ in what they believed influences the construction of their online profiles. In Germany and the US, users were more likely to have claimed that social networking websites influenced their online profile.[415]

Questions 10 and 11 seek to understand whether users have unintentionally posted private information, and what type of information.

> Q10. Have you ever shared something publicly that you intended to keep private? Q11. What type of information did you share publicly?

Results suggest that children were more likely to have unintentionally posted information than adults (27% vs. 17%).[416] For both adults and children, information that was more likely to be shared unintentionally included information about their personal life (56% - not applicable to children), photos of themselves or their family (38% of adults, 36% of children) and their birthday (31%of adults, 34% of children). Additionally, children were more likely to indicate

[411] Ibid., p. 4.
[412] Ibid., p. 10.
[413] Ibid.
[414] Ibid.
[415] Ibid., p. 37.
[416] Ibid., p. 23.

that they had mistakenly shared information about their friends (44% compared to 15% of adults).[417]

Having developed an understanding of how people's online activities potentially influence their online reputations, the study also asked respondents whether they were concerned about their online reputation:

> Q3a. How concerned are you about your online reputation?[418]

Responses indicated that some respondents were concerned about their online reputations: 32% of adults were "somewhat concerned", 23% of adults were "very concerned". Alternatively, 24% of adults indicated that were "not very concerned" and 16% indicated they were "not concerned at all".[419] The majority of children also stated they were concerned about their online reputations; 36% were "somewhat concerned", 23% were "very concerned", 25% were "not very concerned" and 13% stated they were "not concerned at all".[420] Respondents in Spain and Canada claimed they were "very concerned" (31% and 25% respectively).[421] Respondents in the US and Germany claimed to be "not concerned at all" (23% and 17% respectively).[422]

Researchers asked respondents whether they were concerned about the influence of others' actions on their online reputation:

> Q3b. How concerned are you that your online reputation may be harmed by content posted by someone else?[423]

Answers to this question indicate that both adults and children are more concerned about how the actions of others might harm their online reputation: 28% of adults and 30% of children indicated they were "very concerned", 32% of adults and 37% of children indicated they were "somewhat concerned", 22% of adults and 20% of children stated they were "not very concerned" and 14% of adults and 10% of children claimed they were "not concerned at all".[424] Those who were "very concerned" were more likely to be from Spain and Germany (38% and 26% respectively). The least amount of concern was found in the US and Canada (23% and 18% respectively).[425] The inclusion of this question is a useful way of understanding the impact of personal action upon concern of online reputations, since it seems to be the actions of others, rather than personal actions, that cause the most concern.

The interviews then proceeded to ask respondents how much control they felt they had over their online reputation:

> Q5. How much control do you think you have over your online reputation?[426]

---

[417] Ibid.
[418] Ibid., p. 15.
[419] Ibid.
[420] Ibid.
[421] Ibid., p. 39.
[422] Ibid.
[423] Ibid., p. 15.
[424] Ibid.
[425] Ibid., p. 39.
[426] Ibid., p. 15.

Responses to this question differ slightly between adults and children, with children believing they have slightly more control of their online reputation than adults: 18% of children compared to 17% of adults believed they had "complete control" over their online reputations, 55% of children and 49% of adults claimed to have "a lot of control", 26% of adults and 20% of children felt they had "little control" and 4% of adults and 3% of children felt they have no control at all. There were also those who did not know: 5% of adults and 4% of children.[427] Those in Germany and Spain are more likely to claim that they have complete control (19% and 18% respectively). Alternatively, those in Canada and the US are more likely to indicate that they have no control (5%).[428]

In relation to the issue of security, in the form of "harm", the survey included a question asking respondents whether they had experienced "harm" from friends or family, and if so, in what form:

> Q15a. Has a friend or family member ever posted something online that has influenced your reputation either positively or negatively? Q15c. What were the activities that you felt, which negatively influenced your reputation?[429]

Children were slightly more likely to have experienced a negative impact on their reputation via the actions of friends or family (16% vs. 11% of adults).[430] Activities by their friends or family that were likely to influence their reputation were more likely to be from either posting a comment on a social networking website (47%) or from posting a photo of them or family (47%). Activities that were least likely to have a negative influence were others updating their social networking profile (8%).[431] Those in Canada, Ireland or the US were more likely to have experienced a negative influence on their reputation by friends or family through posting a comment on a social networking website, while those in Spain were least likely to have experience this (72%, 69%, 67% and 43% respectively).[432]

As a final area of consideration, the interviews also provide us with an indication of what measures individuals might be taking to manage their online profiles. The survey used the following question:

> Q6. Which of the following steps have you ever taken to manage your online profile?[433]

The most common measures taken by adults and children included: searching for their own name (63% of adults, 61% of children), using privacy settings on a social networking site (51% of adults, 53% of children) and deciding not to post specific text, photos or videos (47% of adults, 48% of children). Respondents were less likely to: employ an online reputation management company (3% of adults, no children), contact a web site owner or administrator to ask them to remove information (8% of adults, 7% of children) or not take any steps (9% of adults, 6% of children).[434] Those who had not taken any steps to manage their online profile were more likely to be from the US or Canada and least likely to be from Spain or Germany

[427] Ibid.
[428] Ibid., p. 41.
[429] Ibid., p. 30.
[430] Ibid.
[431] Ibid.
[432] Ibid., p. 51.
[433] Ibid., p. 19.
[434] Ibid.

(15%, 11%, 6% and 5% respectively).[435] Those who chose to change their privacy settings on a social networking site were more likely to be from Ireland or Canada, and least likely to be from Spain (60%, 56% and 42%).[436] Thus, respondents seem to be more inclined to take measures that they can physically manage themselves, rather than leaving in the hands of others.

4.19.3 *Relationship with other surveys*

Comparing results between this survey and the *PEW Internet & American Life Project: Reputation Management and Social Media* (2007) suggest that individuals outside of the US are also concerned with the effect of having an online profile and what this can imply for their online reputation. This survey has broadened our understanding of how the actions of others can influence attitudes towards the safety of having an online profile. The PEW study in reputation management was somewhat limited to asking whether people had a bad experience on the Internet. As with other surveys assessed in this analysis, some individuals are taking measures to enhance their privacy online. Respondents are more inclined to take measures that they can physically manage themselves, rather than leaving in the hands of others. Finally, a similar study in the US in 2010 by Hoofnagle et al. echoed this survey's findings that young people care about their privacy.[437]

4.19.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages.

The survey has reinforced the notion of individuals taking measures to enhance the privacy of their personal data online. This survey takes a slightly different route to trying to understand the impact of sharing information online from the point of view of an online reputation. The survey has highlighted differences in perceptions between children and adults because of the use of social networking sites and what this means for sharing personal information. There is also a notable difference between different types of online activities and what adults and children think contribute to developing an online profile. In relation to concern, both adults and children showed some level of concern with regard to the amount of information about them that contributes to them having an online reputation. In relation to control of an online reputation, children are more likely to believe they have control than adults. The survey has also found evidence to suggest that both adults and children are taking some measures to manage their profile online.

4.20 INTERNET PRIVACY RESEARCH

The survey on Internet Privacy by the Centre for Critical and Cultural Studies at the University of Queensland was a telephone survey that took place between the 17 November

[435] Ibid., p. 42.
[436] Ibid.
[437] Hoofnagle, Chris, Jennifer King, Su Li and Joseph Turrow, "How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?", *Social Science Research Network*, 14 April 2010. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864

and 14 December 2011.[438] The aim of the survey was to develop a wide understanding of Australian attitudes towards privacy on the Internet. Although limited, this survey focuses on Internet privacy and assists in understanding of measures individuals are taking to enhance their privacy on the web.

4.20.1 *Methodology*

The survey used a random sample of 1016 participants of Australian members of the public over the age of 18.[439] Researchers identified the telephone numbers targeted using a random sample of both landline and mobile phone users in order to gain a more representative sample. As with other surveys, the researchers involved in this survey applied weighting to ensure findings were representative of the wider Australian population, and further information on weighting techniques can be found within the final report.[440]

4.20.2 *Main findings*

The majority (68%) of respondents participating in the survey claimed that they used the Internet on a daily basis; others (14%) indicated they used the Internet several times a week and 13% claimed they had never used the Internet.[441] Thus Australian Internet use is widespread as seen in other surveys included in this analysis.

When identifying whether citizens are taking measures to protect their privacy on websites, the majority of respondents (78%) claimed they had refused to give their personal information to a website. Alternatively, 69% stated that the refused to use an application or website because of its need to acquire personal data, 50% used a nick name or pseudonym and 17% used an incognito function on a web browser.[442] Within each response, those who claimed they had taken this measure were more likely to be younger respondents, those who had higher levels of education and those who used the Internet on a daily basis.[443] These findings suggest that more technical measures such as using an anonymous or incognito function was less likely to be used than more casual responses such as refusing to provide information or use an application. This may be an indication of limitations in a person's knowledge and awareness of such measures.

In order to understand individuals' choice of measures to protect their privacy, researchers also asked respondents how often they read privacy statements online. The survey included the following question, providing respondents with 5 options to choose from (Always/most of the time, sometimes, rarely, never and don't know):

> Thinking now about using an online service, either to sign up to a website or buy a product, how often do you read that websites privacy policy?[444]

When considering the entire sample, the majority of respondents stated that they never read privacy statements (36%); alternatively, 28% claimed they rarely read privacy statements,

[438] Arnott, Christy, *Internet Privacy Research*, The University of Queensland Australia, February 2012, p. 6.
[439] Ibid.
[440] Ibid., p. 7.
[441] Ibid., p. 14.
[442] Ibid., p. 18.
[443] Ibid., p. 18. Note: no statistics were provided.
[444] Ibid., p. 26.

18% stated that they sometimes read them and 18% stated they always read them.[445] In relation to socio-demographic variables, men were slightly more likely than women to have never read privacy statements (37% vs. 34%). Those in the oldest and youngest categories were more likely to not have read privacy statements (75+ - 48%; 18 to 24 year olds – 40%). Education seems to make very little difference in influencing whether people read privacy statements; 36% of those with a university education never read privacy statements, along with 38% that left school after year 11.[446]

In order to understand participants' privacy concerns the survey used the term "privacy", but did not include any indication of what the term meant. The survey included the following question:

> To what extent would you agree or disagree with the statement; the only people who are concerned about their privacy are people with something to hide?[447]

Only 19% of respondents agreed with this statement. With the exception of those who responded with "neither" (4%), 38% disagreed and 37% strong disagreed, showing that the majority of respondents do believe that a privacy is a concern for all, not just for those with something to hide.[448] From a socio-demographic perspective men were more likely to agree with this statement than women (20% vs. 16%), likewise, women were more likely than men to strongly disagree with the statement (43% vs. 38%). Those who were over the age of 65 were more likely to agree with the statement; alternatively, those aged 40-64 were more likely to strongly disagree.[449] Those who spent more time in education were more likely to strongly disagree than those who had only stayed in education up to year 11 (49% vs. 31%).[450]

4.20.3 *Relationship with other surveys*

As with previous surveys this survey also asked about whether individuals read privacy statements. When asking people about their privacy concerns and the measures that people may take, this survey is somewhat limited in the comprehensiveness of questions asked.

4.20.4 *Use of the survey results*

Although the consortium conducted a careful search, we did not find any evidence of comments by policy-makers, or press reports on the survey results. However, it is possible that some reports appeared in print form only, or in other languages.

This survey from Australia has revealed that Australian Internet users are certainly concerned about the privacy of their personal information on the web. The survey also identified that users seem to be taking limited steps to help maintain control over their own data. However, the survey results are somewhat limited, since the instrument did not include adequate questions to fully understand privacy concerns and individuals' measures to enhance their privacy on the Internet.

---

[445] Ibid.
[446] Ibid.
[447] Ibid., p.25.
[448] Ibid.
[449] Ibid.
[450] Ibid.

4.21 CONCLUSION

The primary aim of this task has been to present an analysis of what public opinion surveys on privacy, trust, security and surveillance divulge about citizens' perceptions of each of these four issues. A secondary aim of this task, was to identify, what measures, if any, individuals were taking to enhance their security, privacy and trust. To achieve these aims, partners compiled a data set of 260 surveys relating to privacy, trust, security and surveillance. Partners then selected 20 surveys to conduct a comparative analysis, enabling for a closer examination of public opinion relating to these issues. The results of this analysis have been presented in this chapter. To further understand these findings, partners have conducted a horizontal analysis of these results; the findings can be found in chapter five of this report.

Chapter 5: Horizontal analysis

Hayley Watson, David Wright and Rachel Finn
Trilateral Research & Consulting, LLP

5 HORIZONTAL ANALYSIS

In this chapter, we analyse what we can conclude about each of the four issues from the surveys in this report, helping us to answer questions such as: How does the public feel about their privacy? Are they willing to support increased surveillance measures to enhance their security? Or has the time come where the public are concerned about the impact of surveillance on their privacy? Who do people trust more with the handling of their personal data, public or private companies?

The analysis proceeds in seven sub-sections. The first four sub-sections focus on each of the four themes: privacy, trust, security and surveillance. For each theme, we consider: public attitudes towards these issues, measures taken by citizens to enhance their privacy (for instance) and instances of convergence and divergence across the surveys. Subsequent subsections will focus on demographic, temporal and technological differences.

5.1 PRIVACY

Seventeen of the 20 surveys analysed in detail in this report were helpful in understanding contemporary public opinions of privacy across Europe and elsewhere. The remaining surveys did not include any reference to the issue of "privacy". The following are relevant to this analysis:

Table 11: Existing surveys relating to privacy

Title	Privacy
Eurobarometer 46.1: Information technology and privacy	X
Special 9/11 Poll	X
Urban Eye - CCTV in Europe	X
Survey on citizens trust in ID Systems and Authorities	X
PEW Internet & American Life: Digital Footprints	X
Flash Eurobarometer 225: Citizens' perceptions of data protection	X
Personlig Integritet: Perceptions of privacy in public spaces	X
The Globalization of Personal Data Project	X
Canadians and Privacy	X
Privacy 2.0	X
State of the Nation	X
Unisys Security Index	X
PEW Internet & American Life: Reputation Management	X
EU Kids Online: Risks and Safety on the Internet	X
Special Eurobarometer 359: Data protection and e-Identity	X
Online Profile & Reputation Perceptions Study	X
Internet Privacy Research	X

5.1.1 *Public attitudes towards privacy*

A key aim in this analysis of existing surveys was to try to understand public attitudes towards privacy. The surveys analysed here suggest that many individuals are concerned about their privacy. Findings from the surveys point towards privacy having been a concern that has remained in people's minds over time. For instance, when considering the history of the three Eurobarometer surveys, Europeans have consistently expressed concern about

privacy from 1997 until the present.[451] The following table provides further evidence of concern over privacy being present throughout the surveys:

Table 12: Respondents concerned about privacy

Survey	Respondents concerned about privacy?
Eurobarometer 46.1: Information technology and privacy	Yes
Special 9/11Poll	Not directly asked
Urban Eye - CCTV in Europe	Not directly asked
Survey on citizens trust in ID Systems and Authorities	Not directly asked
PEW - Digital Footprints	Not directly asked
Flash Eurobarometer 225: Citizens perceptions of data protection	Yes
Personlig Integritet: Perceptions of privacy in public spaces	Yes
The Globalization of personal data project	Yes
Canadians and Privacy	Yes
Privacy 2.0	Yes
State of the Nation	Yes
PEW - Reputation Management	Concern lacking
EU Kids Online: Risks and Safety on the Internet	Not directly asked
Special Eurobarometer 359: Data protection and e-Identity	Yes
Online Profile & Reputation Perceptions Study	Yes
Internet Privacy Research	Not directly asked

The above table shows that respondents expressed concerns about privacy in 15 of the 16 privacy-focused surveys, and only one survey found evidence that concern was lacking. Concern over privacy was found to be less by those who used the Internet more often. From a socio-demographic perspective, women reported being slightly more concerned about their privacy than men (for example; *Eurobarometer 46.1: Information technology and privacy* and *Flash Eurobarometer 225: Citizens perceptions of data protection*). Further discussion regarding different demographics can be found in section 5.5.

All (relevant) surveys analysed demonstrated consistency across Europe, in that Europeans are concerned about the privacy of their personal data, although, when comparing two Eurobarometer surveys from 2008 and 2011, as can be seen in figure 34 (below) there has been a decline in those that are "very concerned" over time, but an increase in those that are "fairly concerned".

[451] Further insights into trends over time are identified and discussed in section 3.6.

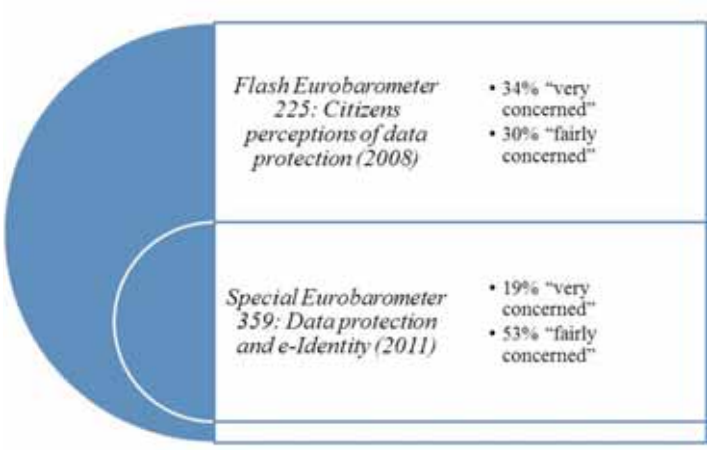


Figure 34: Public Opinion Eurobarometer Surveys – Evidence of concern over privacy of personal data in Europe

Public concern over the privacy of personal data was also found outside of Europe, examples include: Canada, the United States, Australia, Japan and China. Thus, concern over privacy is not simply a European phenomenon, but one that manifests globally.

Some of the surveys included in this analysis have revealed that Internet users are not just concerned about the privacy of their personal information, but at times they are also concerned about the safety of their personal information on the Internet. For instance, the *Flash Eurobarometer 225: Citizens perceptions of data protection* survey revealed that 80% of Europeans were considerably worried about the security of their data on the Internet. Similarly, findings from The Globalization of Personal Data project also identified concern with regard to having to supply personal information on the Internet. However, this contrasts with findings by the *PEW Internet & American life Project: Digital footprints,* where there was evidence of some American participants not being concerned about the amount of information about them online; for them, it was part of everyday life. Accordingly, concern and security may be two separate issues to consider. Further, one could usefully ask if people become so inured to intrusions upon their privacy that over time those intrusions cease to be a concern.

Not only does future research need to explore all seven types of privacy, but in addition researchers should try to explore public attitudes towards privacy of data and image in a more elaborate fashion. It is not sufficient to ask if people are concerned about the privacy of their personal data, particularly when individuals might be willing to share personal information. Rather, researchers should consider the element of security in relation to concerns about privacy. In addition, researchers should consider why respondents are not concerned; this is not a simple "yes" or "no" question, asking why leads to further insights of why that is the case, enabling further understanding to be developed. For instance, the *Canadians and Privacy* survey asked respondents whether they felt they were doing a "good job" at protecting their privacy online. Such a question may be important in trying to understand whether individuals are concerned about their privacy online; however, again, elaboration is required.

5.1.2 *Citizens' measures to enhance privacy*

The final area of consideration in relation to this horizontal analysis of privacy relates to whether citizens are taking measures to enhance their privacy. As illustrated above, many are

concerned about their privacy. Across Europe, surveys such as the *Flash Eurobarometer 225: Citizens perceptions of data protection* and The Globalization of Personal Data *project* show that some individuals are taking measures to try to enhance their privacy. As revealed in the G*lobalization of personal data project* and the *Special Eurobarometer 359: Data protection and e-Identity*, measures that seem to be more favourable include:

- Refusing to provide personal information to companies and government,
- Asking a company not to sell information,
- Asking a company to be removed from their marketing list,
- Reading online privacy policies,
- Avoiding the sharing of their user name and password, and
- Avoiding the disclosure of payment details online,
- Using anti-spyware and
- Deleting cookies.

Less favourable measures to enhance privacy include:

- Purposefully giving false information,
- Asking to see what information is held on record,
- Asking for personal information to be removed,
- Using a dummy e-mail account and
- Shredding information.

Other surveys such as the *PEW Internet & American Life Project: Digital Footprints* have sought to understand specific measures used on social networking sites. For instance, for those with a profile on a social networking site, some were taking measures by changing the visibility of their profiles. In the *EU Kids Online survey*, some children were aware of the importance of taking measures to protect their privacy. These measures were commonly in the form of controlling privacy settings on social networking websites. Future research may want to determine the different measures used for different activities online that involve sharing personal information or data.

Whilst some individuals may be taking measures to enhance their privacy online, there appears to be a limitation in terms of citizens having the appropriate knowledge to know how to protect themselves and manage their privacy in the digital world. For instance, 56% of those surveyed in the *Flash Eurobarometer 225: Citizens perceptions of data protection* claimed they did not know of any tools or technologies that could be used to limit the collection of personal data from their computer. However, this survey did not ask any specific questions that would enable an understanding of the actual measures of which people were aware. As will be discussed in section 5.5, by reviewing a selection of surveys, authors of this report have been able to identify differences in relation to socio-demographics and the measures that people are taking to enhance their privacy.

Future research into this area should consider asking respondents how successful they feel they are in maintaining and managing their privacy as asked by the *Canadians and Privacy* survey. Such a line of questioning would allow researchers to further understand the link between an individual's confidence in their abilities to manage their privacy and whether they take any measures. Proceeding from this, questions could also ask respondents whether they

have had any trouble with privacy data breaches as examined in surveys such as the *Online Profile and Reputation Perceptions Study*.

Currently, our understanding of public attitudes towards issues relating to privacy demonstrates that individuals are concerned about the privacy of their data. As will be seen in section 5.4, individuals are also concerned about surveillance measures that impact the privacy of their communication, the privacy of their bodies, the privacy of their behaviour and the privacy of their locations Furthermore, some individuals are taking measures to protect themselves and their privacy online. Currently our understanding is not entirely adequate; further development of questions used in this research is required to deliver a more accurate insight into the attitudes and perceptions of all seven types of privacy. Only then can policies be developed to help safeguard citizens' privacy.

5.2 TRUST

The review of existing surveys in this report contains a series of nine surveys that included questions regarding whether citizens trust organisations with the handling of their personal data. The following surveys are relevant to this analysis:

Table 13: Existing surveys and trust

Title	Trust
Eurobarometer 46.1: Information technology and privacy	X
Urban Eye - CCTV in Europe	X
Survey on citizens trust in ID Systems and Authorities	X
Flash Eurobarometer 225: Citizens perceptions of data protection	X
The Globalization of personal data project	X
Canadians and Privacy	X
State of the Nation	X
PEW - Reputation Management	X
Special Eurobarometer 359: Data protection and e-Identity	X

5.2.1 *Public attitudes towards trust*

The analysis of existing surveys presented in this report revealed an important insight into who citizens claim they trust with managing their personal data. When considering five of the surveys that looked at trust, as illustrated in the figure below (Figure 35), all of the surveys indicated that individuals were more likely to trust public organisations and institutes over private companies: the *Flash Eurobarometer 225: Citizens perceptions of data protection, Special Eurobarometer 359: Data protection and e-Identity and State of the Nation* identified this in a direct fashion. Additionally, the *Canadians and Privacy* survey found that individuals were distrustful of business organisations with the handling of their data. Likewise, the *PEW Reputation Management* survey found that users did not trust social networking websites (private companies).

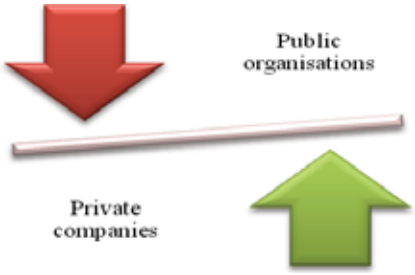


Figure 35: Who individuals are more likely to trust with their data

However, just because evidence points towards individuals trusting public organisations more than private companies, that is not to say that individuals were entirely trusting of public organisations. In fact, findings from surveys such as the *State of the Nation* suggest that some people were also suspicious of public organisations. Additionally, the *URBANEYE: CCTV in Europe project* reveals that some individuals felt that public bodies such as the police should be regulated in their handling of personal data rather than being given a free rein. Similarly, a study by the Department of Health and the NHS in the UK, in 2009, found that individuals do want to have a say, in the form of consent, as to when their personal data is used (for instance, in research); and thus may not be entirely trusting when their data is being used by a public organisation without their permission.[452] Thus, trust in organisations' handling of personal data is not straightforward. Future surveys ought to develop questions that seek to further understand why individuals do not trust certain organisations, and what they feel can be done to improve their trust.

5.2.2 *Citizens' measures to enhance trust*

When considering whether citizens are taking measures to protect their personal data, there was no specific evidence to suggest what measures citizens might be taking with regard to trust. Results from section 3.2 demonstrate that some individuals took steps towards avoiding the disclosure of information to organisations, which indirectly suggests that some individuals are taking measures to help protect their privacy from organisations that they may not trust. Future research should try to directly understand if there are any other measures that individuals might be taking in relation to trusting others with their privacy. It should also seek to understand the other types of privacy and not simply focus attention on privacy of data and images. For instance, surveys may want to ask respondents whether they trust airport officials with the images generated by full body scanners.

Grenville argues that the relationship between citizens' trust and surveillance technologies and those responsible for surveillance technologies is complex and fraught with unequal power relations.[453] Grenville presents the example of mistrust and visual surveillance systems: "You may not trust how CCTV data is being used, but if you want to get on the subway and the only entrance has CCTV, you may feel you have no choice but to give up control over

[452] Research Capability Programme Team, *Summary of Responses to the Consultation on the Additional Uses of Patient Data*, NHS: Connecting for Health, 27 November 2009. http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/documents/digitalasset/dh_109343.pdf

[453] Grenville, Andrew, "Shunning Surveillance or Welcoming the Watcher? Exploring How People Traverse the Path of Resistance", in Elia Zurelik, Lynda L. Harling Stalker, Emily Smith, David Lyon and Yolande E. Chan (eds.), *Surveillance, Privacy and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal and Kingston, 2010, pp. 70–83.

your bodily image".[454] This was reflected in the *Globalization of personal data project*, where researchers asked the following questions:

> When it comes to the privacy of personal information, what level of trust do you have that the (country of interview) government is striking the right balance between national security and individual rights?[455]
>
> What level of trust do you have that private companies, such as banks, credit card companies and places where you shop, will protect your personal information?[456]

Future research should ask more specific questions as to whether individuals trust certain surveillance systems and what this means for the privacy of the person, as well as the privacy of behaviour and action and the privacy of location and space.

Overall, evidence from the surveys analysed in this report suggest that individuals are certainly concerned about trusting others with handling their personal data. The surveys analysed here have not been able to provide a clear link between whether trust of organisations influenced public perceptions towards infringements on privacy, as a result of surveillance technologies to enhance their security. Thus future studies may wish to, consider studies such as that by Pavone and Esposto[457] to fully understand this complex relationship. Furthermore, public authorities seem to be trusted more than private companies. Additional research is required in this area to further understand citizens' attitudes towards trusting others, and what measures can be taken to establish a more trusting relationship between public and private organisations, and the public. Additionally, the relationship between trust and the different types of privacy and surveillance technologies require further attention.

5.3 SECURITY

The review of existing surveys included in this report included 13 surveys that contained questions asking respondents about their attitudes relating to security. The following table (Table 14) lists the relevant surveys:

Table 14: Existing surveys and security

Title	Concerned with security
Special 9/11 Poll	X
A two-edged sword – public attitudes towards video surveillance in Helsinki	X
Urban Eye - CCTV in Europe	X
E-Identity: attitudes towards biometrics	X
Flash Eurobarometer 225: Citizens' perceptions of data protection	X
The Globalization of personal data project	X

[454] Ibid., p. 73.
[455] Ibid., p. 74.
[456] Ibid.
[457] Pavone, Vincenzo and SaraDegli Esposto, "Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security", *Public Understanding of Science,* Vol. 21, No. 5, 2010, pp. 556-572.

Title	Concerned with security
Canadians and Privacy	X
State of the Nation	X
Financial Times/Harris Poll: Body Scanners	X
Unisys Security Index	X
EU Kids Online: Risks and Safety on the Internet	X
Special Eurobarometer 359: Data protection and e-Identity	X
Online Profile & Reputation Perceptions Study	X

5.3.1 *Public attitudes towards security*

The surveys assessed in this report did not provide an indication of how individuals feel about security, and threats to their security, such as that posed by international terrorism. Instead, physical security is commonly discussed in relation to increasing surveillance measures. Findings from some surveys have revealed that individuals are willing to give up some of their privacy, thereby supporting increasing surveillance measures to protect their physical security. This finding was attributable to several surveys, for instance: *Special 9/11 Poll*, *A two-edged sword: video surveillance in Helsinki* and *URBANEYE: CCTV in Europe*. Respondents were particularly more likely to support enhanced surveillance when confronted with the threat of "radical uncertainty" in the form of terrorism (see the following surveys for examples: *Special 9/11 Poll, Flash Eurobarometer 225: Citizens perceptions of data protection, Canadians and Privacy* and *Financial Times/Harris Poll: Body Scanners*).

The use of surveillance measures to aid information security was seen in relation to some individuals supporting new technologies, such as biometrics, to help protect them from threats such as financial fraud; this was found in the *E-Identity: attitudes towards biometrics survey* with more than 50% of respondents from all countries believing that biometrics could help reduce financial fraud. Alternatively, when considering public attitudes towards information security some surveys revealed that individuals are concerned about threats they may face relating to their personal data. For instance, the *Flash Eurobarometer 225* found that a substantial number of Europeans (82%) were concerned with the safety of transmitting data over the Internet. Elsewhere, the *Unisys Security Index* revealed that individuals had moderate concerns with regard to their computers being secure from viruses, unsolicited e-mails, purchasing goods online and online banking. The *Unisys Security Index* also revealed that individuals were most concerned about their financial security. This was perceived as a greater threat than information security.

5.3.2 *Citizens' measures to enhance security*

Although the surveys analysed here were somewhat limited in reporting individuals' security concerns, the surveys have provided some indication of what measures individuals may be choosing to take in order to protect themselves, particularly in relation to information security and physical security on the Internet. Results from the *Flash Eurobarometer 225: Citizens perceptions of data protection* show that there was a lack of awareness among individuals as to the relevant measures that were available to them to help secure their data online. However, as seen in Table 15 (below) some of the surveys analysed in chapter four, such as *The Globalisation of Personal Data,* shed some light on various measures taken by citizens to enhance security on the Internet:

Table 15: Measures citizens take to protect their data online

Measure	Survey findings
Refusing to provide personal information to companies and/or government	Favourable: • *Globalization of personal data project* • *Canadians and Privacy* • *Special Eurobarometer 359: Data protection and e-Identity* • *Internet Privacy Research*
Asking a company not to sell information	Favourable: • *Globalization of personal data project*
Asking a company to be removed from their marketing list	Favourable: • *Globalization of personal data project*
Reading online privacy policies	Favourable: • *Globalization of personal data project*
Avoiding sharing their user name and password	Favourable: • *Globalization of personal data project* • *Special Eurobarometer 359: Data protection and e-Identity*
Avoiding disclosing payment details online	Favourable: • *Globalization of personal data project* • *Special Eurobarometer 359: Data protection and e-Identity*
Using anti-spyware	Favourable: • *Globalization of personal data project*
Deleting cookies	Favourable: • *Globalization of personal data project*
Using a complex password	Favourable: • *Canadians and Privacy*
Looking for a padlock symbol that would indicate they are using a secure site	Favourable: • *Canadians and Privacy* • *Special Eurobarometer 359: Data protection and e-Identity*
Changing privacy settings on a social network website	Favourable: • *PEW Reputation Management* • *EU Kids Online* • *Online Profile & Reputation Perceptions Study*
Protecting from spam mail	Favourable: • *Special Eurobarometer 359: Data protection and e-Identity*
Purposefully giving false information	Less favourable: • *Globalization of personal data project* • *Special Eurobarometer 359: Data protection and e-Identity*
Asking to see what information was held on record	Less favourable: • *Globalization of personal data project* • *Canadians and Privacy*
Asking for personal information to be removed	Less favourable: • *Globalization of personal data project* • *Special Eurobarometer 359: Data protection and e-Identity* • *Online Profile & Reputation Perceptions Study*

Measure	Survey findings
Using a dummy e-mail account	Less favourable: • *Globalization of personal data project* • *Special Eurobarometer 359: Data protection and e-Identity* Favourable: • *Internet Privacy Research* (false user name)
Shredding information	Less favourable: • *Globalization of personal data project* • *Special Eurobarometer 359: Data protection and e-Identity*

Note: Not all surveys asked about the same measures.

As the table above indicates (Table 15), individuals were more likely to take measures that are readily accessible to them, rather than steps that they have to explicitly and actively choose. For example, a popular "data protection" measure taken by citizens is to simply avoid sharing information, rather than a more active measure such as asking for their personal information to be removed. Future research ought to consider the range of measures available to provide a more comprehensive understanding of the choices people make. The surveys analysed here provide little, if any, detail regarding why people choose certain measures.

Results from this secondary analysis of existing surveys have shown us that attention is predominantly focused on three types of security: physical, radical uncertainty and information security. Results from some of the surveys analysed in section two shows that individuals are willing to give up privacy in the name of enhancing their security. The analysis has also revealed that individuals do appear to care about the security of their personal information on the Internet. As a final point, it has been difficult to declare what the most popular measure is that people are taking to enhance their security online; this is largely a result of the discrepancy in questions and responses from which participants had to choose. Future research ought to develop a more comprehensive understanding of the various measures people are choosing to take, or avoiding, and crucially, why they are making these decisions. It is not sufficient to know what they are doing; it is necessary to understand why, and what they are not doing, so that measures can be taken to help support individuals in protecting themselves on the Internet.

5.4 SURVEILLANCE

The review of existing surveys included in this report contained a series of 12 surveys that related to the issue of surveillance. The following table (Table 16) illustrates the relevant surveys included in this report:

Table 16: Existing surveys and surveillance

Title	Surveillance
Special 9/11 Poll	X
A two-edged sword – public attitudes towards video surveillance in Helsinki	X
Urban Eye - CCTV in Europe	X
E-Identity: attitudes towards biometrics	X
Flash Eurobarometer 225: Citizens' perceptions of data protection	X

Title	Surveillance
Personlig Integritet: Perceptions of privacy in public spaces	X
The Globalization of personal data project	X
Canadians and Privacy	X
State of the Nation	X
Financial Times/Harris Poll: Body Scanners	X
Unisys Security Index	X
Special Eurobarometer 359: Data protection and e-Identity	X

5.4.1 *Public attitudes towards surveillance*

In relation to public attitudes towards surveillance technologies in society, eight of the 12 surveys provide evidence that some individuals respond positively to the use of surveillance measures to help enhance their security. Examples of surveys with these findings include*: Special 9/11 Poll* (although support declined over time), *Two-edged sword, URBANEYE: CCTV in Europe, e-Identity, Eurobarometer 225, Globalisation of Personal Data, Financial Times/Harris Poll: Body Scanners* and the *Unisys Security Index.* Elsewhere, a review of existing surveys on public opinion of surveillance cameras in Canada by Deisman, et al. in 2009 found that the majority of surveys analysed in their study revealed that the public were supportive of CCTV.[458]

However, our analysis illustrates that individuals' support of surveillance in the form of CCTV is somewhat contradicted by findings from other surveys. For instance, the *State of the Nation* survey identified that respondents were not entirely supportive of surveillance technologies invading their privacy; rather, individuals' opinions were more likely to be supportive when there was a greater threat to security. Similarly, the *Financial Times/Harris Poll: Body Scanners* survey found that whilst some individuals tended to support enhanced security measures, such as body scanners, to improve airport security, others believed that there was already too much surveillance. Elsewhere, not included in this analysis, findings from a survey by Gill et al. regarding the introduction and implementation of residential CCTV in the UK suggest that residents were optimistic and supportive of the introduction of CCTV prior to its installation in residential areas. However, after installation, the level of support reduced from 81% to 74%.[459] Thus, support does not necessarily always remain constant. In the case of the Gill et al. study, CCTV was expected to reduce victimisation and help reduce worry about crime, but these effects did not materialise. Conflicting views of surveillance technologies are not restricted to CCTV. As will be discussed in section 3.7, comparing different technologies leads to different findings.

Individuals have also claimed that they are somewhat concerned about the impact of surveillance technologies on their privacy. Examples of surveys where this was found include: *URBANEYE: CCTV in Europe, Personlig Integritet: Perceptions of privacy in public spaces* and *Special Eurobarometer 359: Data protection and e-Identity.* Within EU Member States, the *Special Eurobarometer 359: Data protection and e-Identity* shows that those citizens in Greece (54%), Ireland (43%) and Italy (40%) were more likely to claim they were "concerned" about the recording of their behaviour in public spaces than those in Finland

[458] Deisman, Wade, Patrick Derby, Aaron Doyle, Stephane Leman-Langlois, Randy Lippert, David Lyon, Jason Pridmore, Emily Smith, Kevin Walby and Jennifer Whitson, *A Report on Camera Surveillance in Canada, The Surveillance Project*, Surveillance Camera Awareness Network (SCAN), 30 January 2009. http://qspace.library.queensu.ca/bitstream/1974/1906/1/SCAN_Report_Phase1_Final_Jan_30_2009.pdf
[459] Gill et al., 2007, p.319

(17%) and Sweden (12%).[460] Those in Germany (54%), the Czech Republic (53%), Greece (52%) and Lithuania (51%) were more likely to be concerned about the recording of their behaviour in private spaces than those in Finland (21%) and Sweden (19%).[461] In all countries, with the exception of Greece, as can be seen in the figure below, concern was higher in relation to the recording of behaviour in public spaces than in private spaces:

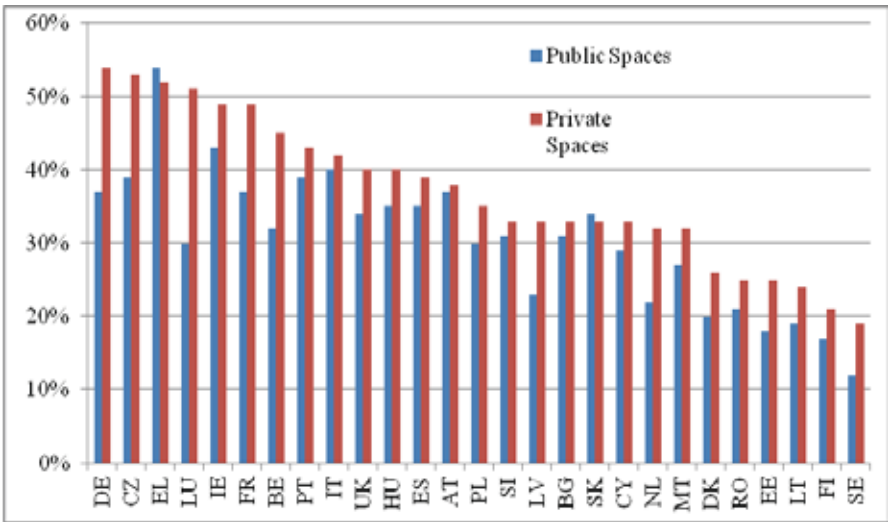


Figure 36: Special Eurobarometer 359: Data protection and e-Identity - Public concern over monitoring of behaviour in public and private spaces[462]

Elsewhere, findings from Gill et al. suggest that individuals do not feel that the presence of surveillance in the form of CCTV invades their privacy.[463] As illustrated in section 5.1, existing surveys do not always try to understand the relationship between surveillance and privacy. Those surveys that do consider this relationship reveal that some individuals care about where surveillance technologies such as cameras are placed (as seen in the *URBANEYE: CCTV in Europe* and *Two-edged sword studies)* and where their images are displayed (as seen in the *Personlig Integritet: Perceptions of privacy in public spaces* study). Members of the public appear to favour the use of surveillance cameras in public rather than private spaces. Additionally, as identified in *Personlig Integritet: Perceptions of privacy in public spaces*, citizens favour the display of CCTV footage in public spaces rather than in the private realm. Similarly, Pavone and Esposto (2010) found that in their investigation into the relationship between security, surveillance technologies and privacy to Spanish citizens, that there were some individuals that were sceptical of the effectiveness of surveillance technologies, and that there was a preference for surveillance to occur in public spaces rather than private spaces.[464] Furthermore, Pavone and Esposto found that the traditional trade-off model between privacy and security was not straightforward. They found that trust was an important factor in determining whether individuals felt that trading privacy for security was effective: those citizens that did not trust governments' surveillance measures were concerned about their privacy, and felt that their privacy had been infringed without their security being enhanced. Alternatively, those that trusted governments were more inclined to feel that their security had been increased without having their privacy infringed.[465]

[460] TNS Opinion and Social, 2011, p. 72.
[461] Ibid. p. 70.
[462] Ibid., pp. 70-72.
[463] Gill et al., 2007, p. 321.
[464] Pavone and Esposti, 2010.
[465] Ibid.

Whilst some individuals claim that they support the presence of surveillance technologies in their lives to help enhance their security, some also believe that the use of surveillance measures by organisations and companies should be limited. Thus, three surveys mention the regulation of surveillance technologies: *URBANEYE: CCTV IN EUROPE, Flash Eurobarometer 225: Citizens perceptions of data protection* and *State of the Nation.* Control being placed on organisations and institutions' use of these systems provides individuals with an opportunity to enhance their privacy, since few other measures are available to them.

5.4.2 *Citizens' measures to avoid surveillance*

The surveys included in this analysis do not provide an opportunity to understand what measures citizens might take to avoid surveillance in society. This may be a result of surveillance being considered "part of everyday life" as postulated in *A two-edged sword: video surveillance in Helsinki*. None of the surveys assessed in this report included a question relating to this issue; hence, this represents a potential issue for consideration in future research in this field.

Surveys analysed in this report demonstrate that whilst individuals accept the presence of surveillance technologies and support them in their ability to enhance security, there are those that feel that surveillance may pose a threat to their privacy. The surveys have also shown that some individuals feel that organisations and companies should be controlled in their employment and use of surveillance technologies, suggesting a lack of trust towards organisations in relation to surveillance technologies. A series of technological differences emerge in relation to public attitudes towards surveillance; this will be discussed further in section 5.7. Further research ought to try to understand whether there are any measures that individuals can take to help enhance their privacy in the wake of the surveillance society. As discussed in section 5.1, future research should aim to understand the relationship between public perceptions of different types of surveillance technologies and what this implies for people's sense of privacy.

5.5 DEMOGRAPHIC DIFFERENCES

A horizontal analysis of existing surveys regarding public attitudes towards privacy, trust, security and surveillance has revealed interesting insights with regard to both convergence and divergence across the surveys. It provides clues to assist an understanding of the broad social attitudes towards these four issues as well as any similarities and differences in public attitudes according to socio-demographics. Accordingly, this section will consider the four issues: privacy, trust, security and surveillance in relation to location (country), gender, age and education.

Privacy
As seen in section 5.1, citizens across Europe (and beyond) have expressed concern about the privacy of their personal data. Different surveys found varying results in relation to where a person is from and how concerned they are. The one country that seems to be consistent in being least concerned is the Netherlands (with the exception of *Eurobarometer 46.1: Information technology and privacy*, which could point to a change in perceptions over time. This will be explored further in section 5.6). The following table (Table 17) provides further information regarding these findings:

Table 17: Country and concern over privacy

Survey	Most concerned	Least concerned
Eurobarometer 46.1: Information technology and privacy	The Netherlands and the UK	Greece, Portugal and Italy
Flash Eurobarometer 225: Citizens perceptions of data protection	Austria and Germany	Bulgaria, the Netherlands and Czech Republic
Globalisation of Personal Data	Brazil and Spain	Hungary and France
Special Eurobarometer 359: Data protection and e-Identity	Lithuania, Ireland, Portugal and Greece	Sweden, the Netherlands and Malta
Online Reputation Management	Spain and Canada	the USA and Germany

As the table above shows, each of the surveys included different countries in their sample, thus determining a cohesive understanding of concern across countries is somewhat difficult, causing results to be inconclusive. Section 5.6 will consider trends over time, where some surveys included in this analysis have provided an understanding of trends over time for the countries they have surveyed.

When we consider public concern over privacy according to gender, evidence across three of the surveys suggests that women are slightly more worried about the privacy of their personal data than men. The following figure provides further information to support this finding:

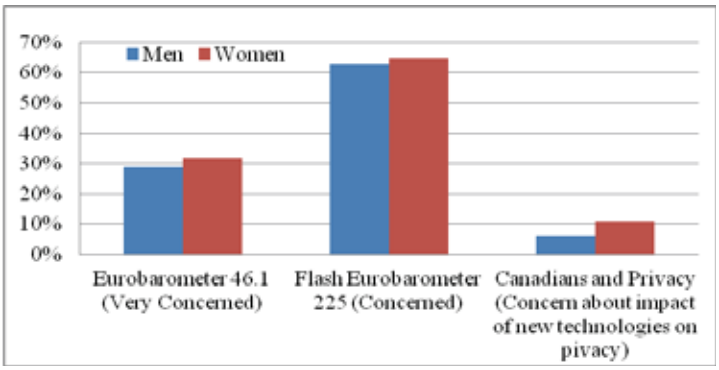


Figure 37: Gender and privacy

This level of (slightly) more heightened concern among women is also evident when considering the actions of individuals. For instance, when considering the *EU Kids Online* survey, girls were more likely to report keeping their profiles on a social networking site private. In contrast, the *Special Eurobarometer 359: Data protection and e-Identity* found no difference in result according to gender for whether individuals are concerned about the risk of the disclosure of their personal information taking place without their knowledge.

In considering measures that individuals may have taken to protect their privacy, findings from both the *Canadians and Privacy* study and the *Special Eurobarometer 359: Data protection and e-Identity* found that men were more likely than women to take measures to protect their privacy.

Noticeable differences in perceptions of privacy in relation to a person's age were also evident. Four surveys (*Eurobarometer 46.1: Information technology and privacy, Flash Eurobarometer 225: Citizens perceptions of data protection, Canadians and Privacy* and *Special Eurobarometer 359: Data protection and e-Identity*) demonstrated that the older the person is, the more likely they are to be concerned about their privacy. This is not to say that young individuals are not concerned, simply that they report less concern than older individuals. This further corresponds with the actions reported by individuals. For instance, when considering the findings from the *PEW Internet & American Life: Digital footprint* survey, teenagers were more likely than adults to set their social network profile privacy settings to ensure greater privacy, in that their profile was not visible to others. Accordingly, since young people take greater control of their information privacy, this may lead to this group being less concerned.

Our analysis also found differences in privacy concerns in relation to education. With the exception of *Eurobarometer 46.1: Information technology and privacy*, in both the *Flash Eurobarometer 225: Citizens perceptions of data protection* and the *Special Eurobarometer 359: Data protection and e-Identity*, findings suggest that the longer an individual spends in education, the more concerned they are likely to be about their privacy. When considering education in relation to whether individuals are likely to take measures to enhance their privacy, one finds that the longer an individual spends in education, the more likely they are to take measures (*Canadians and Privacy, Special Eurobarometer 359: Data protection and e-Identity).*

Trust

The review of existing surveys revealed that there were some differences in responses regarding where individuals are from and whether they trust others with the handling of their personal information. According to both the *EU Survey on Citizens Trust* and the *Flash Eurobarometer 225: Citizens perceptions of data protection,* those in Central and Eastern Europe were less trusting than those in the UK and Ireland (*EU Survey on Citizens Trust),* Denmark, France and the Netherlands (*Flash Eurobarometer 225: Citizens perceptions of data protection).*

The review of existing surveys did not reveal any differences in responses in relation to gender and citizens' views concerning trusting others with their personal data. For instance, both the *Eurobarometer 46.1: Information technology and privacy* and the *Flash Eurobarometer 225: Citizens perceptions of data protection* found no difference in perceptions relating to trust; rather, both men and women felt that their personal data should be protected. The only noticeable difference was the *Special Eurobarometer 359: Data protection and e-Identity*, where women reported being slightly more trusting of public organisations than men, and men reported being slightly more trusting of private organisations than women.

The relationship between age and trust is somewhat clearer. All six surveys that included an insight into trust found that young people were more trusting in relation to giving others their personal information than older participants. For instance, in the *Special Eurobarometer 359: Data protection and e-Identity,* younger respondents reported being more trusting of both public and private organisations than their older counterparts.

When considering the impact of education on trust, the *Flash Eurobarometer 225: Citizens perceptions of data protection* found evidence that the longer an individual spent in education, the more trusting they were of organisations' abilities to handle their personal data.

Security

As with public attitudes towards privacy, it is difficult to understand the differences in public security concerns across different countries. The analysis of existing surveys revealed that individuals in some countries were more concerned about security than others, but there is no clear picture. For instance, the *Unisys Security Index* found that those in Brazil and Mexico were more concerned about their security than those residing in other countries.

The same, however, cannot be said with regard to gender. As revealed in the *Flash Eurobarometer 225: Citizens perceptions of data protection,* women were slightly more likely to indicate that their data was not secure when being transmitted over the Internet. Similarly, men were slightly more confident in taking measures over securing their data on the Internet than women, which provides some indication as to why women may be more concerned than men about the security of their personal data online.

The review of existing surveys identified differences in perceptions about the security of personal data in relation to age. The *Flash Eurobarometer 225: Citizens perceptions of data protection* demonstrated that older respondents were less confident about transmitting their data over the Internet than younger respondents. This may again be linked to younger respondents' having more confidence and being more likely to take measures to secure their personal data on the Internet than older citizens.

This report also found differences in perceptions about the security of personal data in relation to education. As seen in the results of the *Flash Eurobarometer 225: Citizens perceptions of data protection,* those that had spent more time in education were less concerned about the security of their personal information online; they were also more likely to take measures to protect their personal data.

Surveillance

As with the discussion relating to socio-demographics and their impact on perceptions of security, the surveys included in this analysis did not contain many questions that enhance our understanding of the impact of socio-demographics on surveillance. The exception to this is the *Flash Eurobarometer 225: Citizens perceptions of data protection,* which revealed clear patterns in relation to perceptions of surveillance and socio-demographics. For instance, as noted in this report, those who objected to the monitoring of personal data with regard to the threat of international terrorism were likely to be male and higher-educated.

The results of this analysis of the impact of socio-demographics on privacy, trust, security and surveillance have revealed that in relation to some issues different socio-demographic variables have a noticeable impact on public attitudes. There is, however, the problem of surveys failing to consider the impact of socio-demographic variables in relation to public attitudes towards security and surveillance. Further research in this area should make more of an effort to take into account the impact that variables such as gender, age and education can have on attitudes; only then can we begin to understand the needs of different groups in society.

5.6 TEMPORAL DIFFERENCES

Three of the surveys included in this analysis provide an opportunity to understand how citizens' perceptions have changed over time in relation to privacy, trust, security and surveillance. They do so by including past results from their previous surveys in their analysis. These surveys include the *Flash Eurobarometer 225: Citizens perceptions of data protection, Canadians and Privacy* and the *Unisys Security Index.*

Both the *Flash Eurobarometer 225: Citizens perceptions of data protection* from 2008 and *Canadians and Privacy* survey from 2009 provide evidence of concern over privacy changing over time. In particular, the *Flash Eurobarometer 225: Citizens perceptions of data protection* allows concern to be measured back to 1991.[466] When considering all European states that had been included in the Eurobarometer analyses, reported concern over privacy of personal data was relatively high in 1991, with 66% of Europeans reporting concern. This level of concern decreased to 58% in 1996, and then began to increase to 60% in 2003, rising again to 68% in 2008. These trends are evident in the figure below:

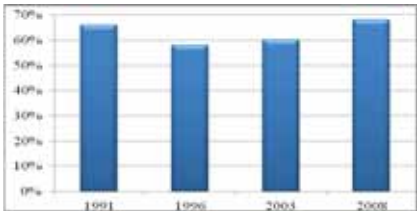


Figure 38: Privacy concerns in Europe over time[467]

Similar results with regard to changes in privacy concerns over time have also been observed by Best et al. in their study of US surveys between 1990 and 2006, where they found that over time, privacy concerns have increased. Additionally, as partners have observes in the present study, Best et al. also recorded a lull in privacy concerns between 2001 and 2003, where concerns over the threat of terrorism in the US resulted in a period of time in which US citizens were willing to forgo some of their civil liberties to help combat the threat of terrorism, however, following this brief period, as also observed in this study, privacy concerns have increased in the US since 2003.[468]

In some countries, there has been a gradual decline from 1991 to 2008: Belgium (56% to 52%), Greece (77% to 67%), France (75% to 70%), Italy (77% to 51%), the Netherlands (54% to 32%) and Sweden (86% to 75%). In other countries, there has been a noticeable increase in levels of concern from 1991 to 2008: Denmark (44% to 73%), Germany (61% to 86%), Spain (37% to 65%), Luxembourg (62% to 66%), Austria (38% to 86%), Portugal (48% to 71%), Finland (30% to 35%). In the United Kingdom, concern remains at 76% as it was in 1991 (with some fluctuation over time).[469] When focusing on more recent trends (between 2003 and 2008) and breaking down concern between different EU Member States, some have experience greater increases than others, whilst others have experience a reduction in concern. The following figure provides further evidence of these trends:

[466] The Gallup Organization, 2008, p. 7.
[467] Ibid., p. 8.
[468] Best et al., 2006.
[469] The Gallup Organisation, 2008, p.8.

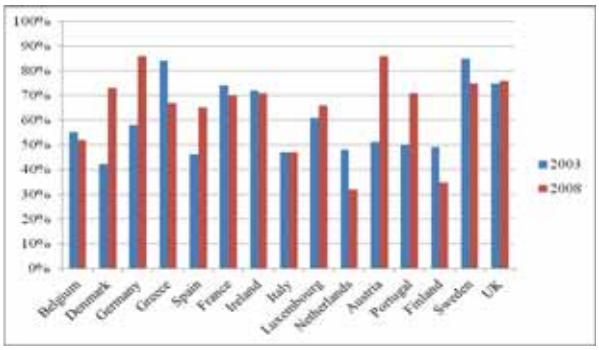


Figure 39: Flash Eurobarometer 225: Citizens perceptions of data protection - Concern about data privacy by organisations that hold personal data[470]

As displayed in the figure above, data from the *Flash Eurobarometer 225: Citizens perceptions of data protection* demonstrates that those in Denmark, Germany, Spain, Austria and Portugal have experienced a vast increase in citizens being concerned about the privacy of their data by organisations that hold personal data. Alternatively, those in Greece, the Netherlands, Finland and Sweden have seen a recognisable decrease in public concerns over the handling of personal data by organisations. Countries such as Belgium, Luxembourg and the United Kingdom have experience minor changes in public concern, whilst concern in Italy has remained unchanged.

The *Canadians and Privacy* survey also identified increases in privacy concerns. There was evidence to show that individuals did not have enough knowledge about the impact of new technologies on their privacy, resulting in this lack of knowledge enhancing their concern about privacy.[471] The change in levels of concern over the privacy of personal data varies in different EU Member States.

In addition to measuring privacy concerns over time, the *Flash Eurobarometer 225: Citizens perceptions of data protection* also offers the opportunity to understand citizens' trust towards organisations responsible for the protection of their data.[472] First, let us consider the differences in trust towards public organisations over time:

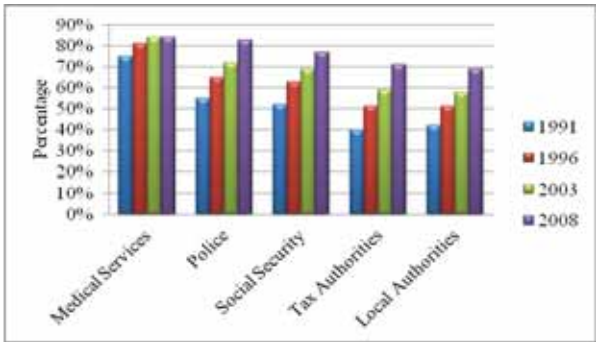


Figure 40: Citizens trust of public organisations in the handling of their personal data over time[473]

[470] Ibid.
[471] EKOS Research Associated Inc., 2009, p. iv.
[472] Ibid., p. 18.
[473] Ibid., p. 18.

As the figure above demonstrates, there has been an increase in trust towards public organisations' abilities to manage citizens' personal information over time. As of 2008, individuals were more likely to trust medical services and doctors with their personal information than local authorities (although levels of trust are still m 50%). As of 2008, those trusting medical services are more likely to be from Denmark (93%) and France (93%); they are least likely to be from Italy (77%) and Greece (67%).[474] Over time, trust towards medical companies has increased in all countries, with the exception of Greece (72% to 67%) and the UK (91% to 86%). Those in Greece (55%) and the UK (61%) are most likely to distrust local authorities. Support for local authorities is higher in Denmark (87%) and Finland (84%).[475] Trust towards local authorities has increased in all countries since 1991. Although they are not trusted as much as public organisations, this increase in trust towards public organisations is also evident with the majority of private organisations:

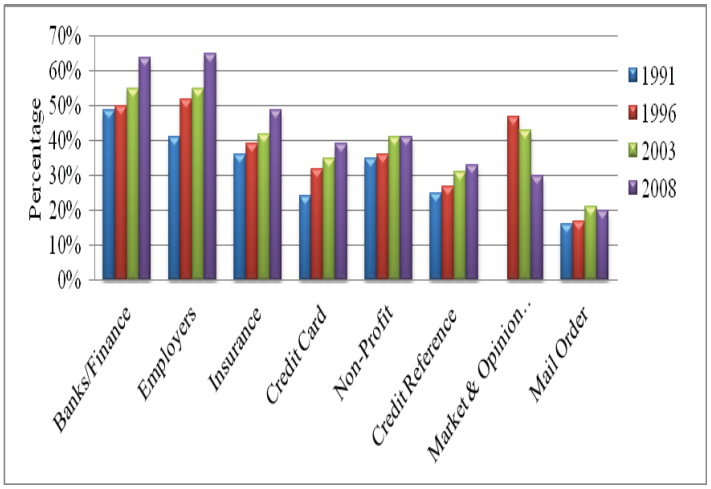


Figure 41: Citizens trust of private organisation in the handling of their personal data over time[476]

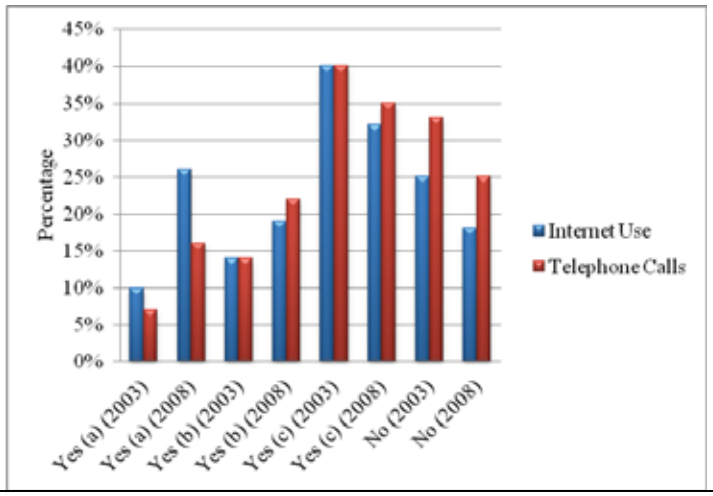
As the figure above illustrates, in 2008, employers were most likely to be trusted by individuals. The least trusted group were mail order companies. Those in Denmark were most trusting of employers (81%), while those in Spain were least trusting of employers (34%). Interestingly, market opinion and research companies are the only type of company that have seen a decline in trust over time; from 47% in 1996 to 30% in 2008. What the survey does not tell us is why there are such significant differences in opinions between countries.

Flash Eurobarometer 225: Citizens perceptions of data protection provides us with an understanding of how users have changed in their knowledge and usage of tools or technologies that improve the security of their data over time. When considering all states included in the analysis, knowledge and use of tools and technologies to improve data security has increased: in 2003, 72% of individuals claimed they were not aware of technologies they could use to enhance the security of their data. This percentage has reduced to 57% in 2008. Likewise, use of technologies has increased: from 6% in 2003 to 25% in 2008. The percentage of individuals who know about technologies, but do not use them has reduced by 1% from 18% in 2003 to 17% in 2008.[477] Countries that have seen a significant reduction in people not being aware of technologies to enhance the security of their data

[474] Ibid., p.58.
[475] Ibid., p. 61.
[476] Ibid., p. 45.
[477] Ibid.

include: Finland (81% to 52%) and Portugal (81% to 34%). Countries where people's awareness of technologies that can support them in securing their data has remained relatively stable. These include Ireland (75% to 71%) and Sweden (58% to 57%). Countries that have seen significant increases in the number of individuals using technologies to enhance their data security include the Netherlands (12% to 44%), Denmark (13% to 48%) and the UK (6% to 37%). Countries that have seen less dramatic change in use of technologies include Ireland (3% to 14%) and Sweden (14% to 25%). Thus, individuals in some countries are becoming more knowledgeable and positive in their use of technologies to enhance the security of their data, while others are not making as much progress. In part, this corresponds to findings from the *Canadians and Privacy* survey, which suggests a growth in Canadians believing they are doing a better job of taking care of their own privacy on the Internet from 2006 to 2009.[478]

As a final area of consideration, the *Flash Eurobarometer 225: Citizens perceptions of data protection* provides us with an indication of changing public attitudes towards surveillance measures over time:[479]



Yes (a) – In all cases
Yes (b) – Yes, but even suspects should only be monitored under the supervision of a judge or with equivalent safeguards
Yes (c) – Yes, but only people who are suspected of terrorist activities

Figure 42: Public attitudes towards surveillance over time[480]

Figure 42 (above) provides evidence to confirm that a significant number of individuals do not support the use of Internet and telephone monitoring to enhance security. In their US based studies, Katz and Tassone[481] and Best et al.[482] also identified high levels of concern regarding the privacy of people's communication. As identified in figure 24, citizens appear to hold greater opposition to the monitoring of telephone calls than Internet use. Across Europe, those that completely oppose the monitoring of both Internet and telephone use has declined. However, between 2003 and 2008 there has been an increase in the number of individuals who feel that "Yes in all cases", individuals' communication should be monitored. However, there is a greater number of individuals that feel that only those suspected of

[478] EKOS Research Associated Inc., 2009, p. 7.
[479] The Gallup Organisation, 2008, p. 51.
[480] Ibid., pp. 51-53.
[481] Katz and Tassone, 1990.
[482] Best et al., 2006.

terrorist activities should be monitored, compared to everyone being monitored. Thus, privacy infringements are not fully supported to enhance security.

Across EU Member States, opposition (those who answered 'no') towards the monitoring of telephone calls was greatest in Ireland (50%), Slovenia (41%), Greece (38%) and Cyprus (38%). Support for the monitoring of telephone calls in all cases was greatest in Malta (29%). Those in Bulgaria (45%), Finland (43%), Italy (43%), the Netherlands (42%), Sweden (42%) and Portugal (42%) were more inclined to state that telephone monitoring was only suitable for those that were suspected of terrorist activities.[483] When considering public attitudes towards the monitoring of people's Internet usage, as of 2008, opposition (those who answered 'no') was greatest in Ireland (31%), Greece (24%), Sweden (23%), the UK (22%) and Denmark (21%). Those in the Netherlands (40%), Finland (39%), Belgium (38%) and Sweden (35%) were more likely to state that the monitoring of Internet use was only suitable for those that were suspected of terrorist activities.[484]

In addition to the *Flash Eurobarometer 225: Citizens perceptions of data protection* and the *Canadians and Privacy* surveys, the *Unisys Security Index* provides an insight into trends over time. Insights into perceptions of threats towards security have changed. For instance, individuals appear to be most consistently concerned with bank card fraud and identity theft than any other threat. Concern over financial security has increased between 2009 and 2010 in Brazil, Germany, New Zealand, UK, Belgium and the Netherlands.[485] Between 2007 and 2010, concern over all other threats, with the exception of national security, has decreased.[486] There has been a reduction in national security concerns between 2007 and 2010 in several countries: Australia, Belgium, Brazil, the Netherlands and the UK. Concern over personal security has decreased in some countries, Australia, Belgium, Brazil, the Netherlands, the US, but has increased in others (e.g., New Zealand).[487] Over time, concern about Internet security has declined in all countries with the exception of Germany and New Zealand.[488] In other countries, there has been an increase in concern over time (e.g., New Zealand and Spain).[489]

These insights into changes in public attitudes over time are useful in directing attention towards matters that require further focus, particularly if there are noticeable differences such as a growing increase in distrust towards local authorities in the handling of personal data. Trends in public attitudes can be useful in directing policy recommendations.

5.7 TECHNOLOGY DIFFERENCES

As time has progressed, so has the number and variety of technologies with which individuals are faced. Technologies range from the Internet, communication devices, such as mobile phones, visual surveillance technologies, such as CCTV or body scanners, location recognition technologies, biometric technologies as well as others. The European Commission-funded SAPIENT project developed a taxonomy of six types of surveillance technologies: visual surveillance, dataveillance, biometrics, communications surveillance,

[483] The Gallup Organisation, 2008, p. 52.
[484] Ibid., p. 51.
[485] Lieberman Research Group, 2012, p. 12.
[486] Ibid., p. 11.
[487] Ibid., p. 18.
[488] Ibid., p. 20.
[489] Ibid., p. 15.

sensors and location determination technologies.[490] Our analysis of existing surveys demonstrates that the surveys we analysed were largely focused on four of these types of surveillance technologies:

- Visual surveillance – Surveillance technologies in areas such as CCTV, UAVs (unmanned aerial vehicles), imaging scanners and satellites.
- Dataveillance – Surveillance based on electronic data traces including: data mining and profiling, data integration: data warehouses, data marts, data federation and cyber surveillance.
- Biometrics – Characterised by the measurement and analysis of human body characteristics to identify or distinguish between individuals. Examples include fingerprints, DNA, facial recognition, iris recognition systems and behavioural biometrics.
- Communication surveillance – The remote interception of telephone and electronic communications. Examples include wiretapping (electronic eavesdropping) of telephone lines, mobile phones, voice-over-IP, call logging and monitoring text-based communication (instant messaging or e-mail).
- Location determining technologies – Location determination systems that use signals to triangulate a location, sense proximity or conduct scene analysis. Examples include GPS, Wi-Fi, cell phone, RFID.[491]

The following surveys considered these types of surveillance technologies:

Table 18: Types of surveillance technologies and existing surveys

Type of surveillance technology	**Existing surveys**
Visual surveillance	• *Special 9/11 Poll* • *A two-edged sword – public attitudes towards video surveillance in Helsinki* • *Urban Eye - CCTV in Europe* • *Personlig Integritet: Perceptions of privacy in public spaces* • *The Globalization of personal data project* • *Special Eurobarometer 359: Data protection and e-Identity*
Dataveillance	• *e-Identity: attitudes towards biometrics* • *Flash Eurobarometer 225: Citizens perceptions of data protection* • *Canadians and Privacy* • *Special Eurobarometer 359: Data protection and e-Identity*
Biometrics	• *Special 9/11 Poll (indirectly)*[492] • *State of the Nation* • *Financial Times/Harris Poll: Body Scanners* • *Unisys Security Index*
Communication surveillance	• *Special 9/11 Poll* • *Flash Eurobarometer 225: Citizens perceptions of data protection* • *Special Eurobarometer 359: Data protection and e-Identity*
Location determining technologies	• *The Globalization of personal data project* • *Special Eurobarometer 359: Data protection and e-Identity*

[490] Bellanova, et al., 2012.
[491] Ibid., pp. 23-53.
[492] Discusses national ID systems which could involve use of fingerprints.

As Table 18 demonstrates (above), the 20 surveys analysed in this report consider five out of the six types of surveillance technologies; attention was not directed towards sensor technologies. Our analysis of existing surveys has revealed that the type of surveillance technology under discussion has an impact on public attitudes towards surveillance. Specifically, members of the public in Europe and the US report wide-spread support for CCTV surveillance as demonstrated by the *Two-edged sword: video surveillance in Helsinki, URBANEYE: CCTV in Europe* and *The Special 9/11 Poll* surveys. In contrast, both the *Special 9/11 Poll* and the *Special Eurobarometer 359: Data protection and e-Identity* report considerable opposition to being monitored by devices or applications that monitor or record their activities online or their mobile phone and e-mail use. Furthermore, the *Flash Eurobarometer 225: Citizens perceptions of data protection* and the *Special Eurobarometer 359: Data protection and e-Identity* also found that individuals are quite concerned about the monitoring of their financial transactions. According to the *Special Eurobarometer 359: Data protection and e-Identity,* those in Greece (67%), the Czech Republic, France (both 64%), Ireland (63%) and Germany (62%) were likely to indicate that they were "concerned" about their behaviour being tracked via payment cards. Alternatively, those in Nordic countries, including Sweden (62%), Finland and Denmark (each 60%), and in Estonia (59%) were likely to claim they were "unconcerned".[493]

These strong attitudes stand in contrast to the "mixed" feelings respondents report in relation to biometrics or other surveillance measures that target the human body and therefore invade privacy of the person. As revealed in the *E-Identity: attitudes towards biometrics Survey*, some individuals answered that biometrics, such as fingerprint scanners, are more secure than the use of a signature for identity purposes. However, this did not mean that respondents necessarily supported the introduction of such measures. There are also mixed feelings with regard to the use of full body scanners to aid security at airports. The *Financial Times/Harris Poll: Body Scanners* demonstrated that those in Great Britain, France and the US are more likely to fully favour body scanners than those in Spain, Germany and China.

Results from this analysis of existing surveys on public attitudes towards the impact of different technologies on privacy concerns suggest that the technology involved as well as the target of the surveillance measure heavily influence peoples' level of support for them.

5.8 CONCLUSION

The PRISMS project involves analysing the traditional trade-off model between privacy and security and devising a more evidence-based perspective for reconciling privacy and security, trust and concern. The primary aim of this chapter has been to provide a horizontal analysis of these issues in relation to demographic, temporal and technological differences and similarities.

This report has indicated a number of conclusions about citizens' understandings of privacy, trust, security and surveillance. The partners' comparative analysis of surveys demonstrates that surveys tend to over-rely upon certain aspects of privacy (e.g., privacy of data and image) and neglect others (e.g., privacy of thoughts and feelings and privacy of association). Findings from the surveys point towards citizens having been consistently concerned about privacy from 1997 to the present. Additionally, the comparative analysis conducted by the partners

[493] TNS Opinion and Social, 2011, p.65.

revealed that as identified by some surveys, individuals are concerned about the impact of surveillance technologies on their privacy. In addition, all European Member States show some degree of hesitation over who should be placed under certain types of surveillance, such as communication. Partners found that surveys did not always ask individuals about their opinion of the impact of surveillance technologies on privacy. The partners found that some individuals are taking measures to enhance their privacy. Examples of favourable measures include refusing to provide personal information to companies and government, asking a company not to sell information, avoiding the sharing of their user name and password and using anti-spyware. Examples of less favourable measures to enhance privacy include: purposefully giving false information, asking to see what information was held on record and shredding information. Reasons as to "why" these options were more or less favourable were not provided.

Partners found that in the surveys analysed in this task, trust is often questioned in relation to the privacy of data and images, where individuals are asked whether they trust others to secure their personal data. In general, individuals claim that they are not entirely trusting of others' ability to correctly handle their personal data. Individuals were more likely to trust public organisations and institutes more than private companies. Partners found that the surveys were somewhat limited in their attempts to understand what measures individuals were choosing to take in relation to enhancing their trust of others. Of the surveys that did investigate measures, a popular measure selected by individuals was to avoid disclosing information.

The partners' comparative analysis of surveys indicates that in addition to over-relying on one particular type of privacy, surveys tend to also over-rely upon certain aspects of security (e.g., physical security and information security) and neglect others (e.g., political security and cultural security). The surveys assessed here commonly focus their attention on discussing security in relation to privacy and surveillance. Partners have found that surveys indicate that some members of the public are willing to sacrifice some privacy to achieve greater security; however, this is only within certain limits. The surveys have provided some indication of what measures individuals choose to take in order to protect themselves online; respondents were particularly attracted to measures that were readily accessible, rather than more practical steps that they would have to explicitly and actively choose. For instance, respondents would prefer to refuse to provide personal information to companies or the government than asking for their personal information to be removed.

In relation to public attitudes of surveillance technologies in society, surveys often directly refer to the term "surveillance" and tried to develop a wider understanding of the terms meaning by providing examples of surveillance technologies such as CCTV cameras. The surveys analysed in this task provide evidence that some individuals respond positively to the use of surveillance measures to help enhance their security. Whilst some individuals claim that they support the presence of surveillance technologies in their lives to help enhance their security, others believe that the use of surveillance measures by organisations and companies should be limited due to privacy concerns. In particular, all Europeans, with the exception of Greece, claim that they are more opposed to surveillance in private spaces than in public spaces. The comparative analysis has revealed that surveys do not always try to understand the relationship between surveillance and privacy. However, those surveys that do consider this issue have found that people are often uncomfortable with technologies that intrude upon the privacy of their bodies (e.g., biometrics, DNA, body scanners) and privacy of their communications (e.g., e-mail and telephone monitoring). Respondents were also concerned

about where visual surveillance technologies such as CCTV cameras are placed and where their images are displayed. The surveys did not provide any opportunity to understand what measures citizens might take to avoid surveillance technologies; this may be a result of surveillance being considered "part of everyday life".

In addition to assessing what surveys suggest about privacy, trust, security and surveillance, this task's horizontal analysis also involved assessing demographic, temporal and technological differences. The surveys demonstrate that variables such as location, gender, age and education have had a noticeable impact on public attitudes. For instance, younger participants were found to be more trusting of divulging personal information than those older participants. Alternatively, location did play a role in relation to public attitudes concerning trusting others with their data. For example, those in Central and Eastern Europe were found to be less trusting than those in the UK and Ireland, Denmark, France and the Netherlands. In relation to temporal differences, the surveys reveal that citizens' concern over privacy has increased gradually over time; however, people appear to be developing greater trust in the ability of both private and public organisations to manage information. One key temporal difference is that people do not have enough knowledge about the impact of new technologies on their privacy, resulting in this lack of knowledge amplifying their concern about privacy. Finally, as mentioned above, this analysis has revealed that the type of surveillance technology under discussion has an impact on public attitudes towards surveillance, and the technology involved as well as the target of the surveillance measure heavily influence people's level of support for them. For instance, individuals are commonly found to be opposed to the monitoring of their communication, yet, opposition is greater in relation to telephone surveillance than Internet surveillance.

This analysis of surveys has revealed that future research needs to explore all seven types of privacy, and that researchers should try to ask why respondents are or are not concerned with different types of privacy. In future, research should also try to understand the various measures that people may be choosing, or not choosing, to enhance their privacy. Crucially, researchers ought to address why people are making these decisions. Future research should also aim to understand the relationship between public perceptions of different types of surveillance technologies and what this implies for people's sense of privacy. This analysis also indicates that surveys tend to over-rely upon whether individuals trust different organisations in handling their personal data, and should seek to develop a wider understanding of trust in relation to other factors, such as trust of surveillance technologies, as this may influence perceptions relating to different types of privacy. Future research should try to directly understand if there are any other measures that individuals might be taking in relation to trusting others with their privacy, in relation to the various types of privacy, not simply the privacy of their data. As a final point, researchers ought to try to develop a more comprehensive understanding of the various measures people are choosing to take, or avoiding to take to enhance their security and, crucially, why they are making these decisions.

The results of this research will be used to help inform a second task, reported in section five, relating to a meta-analysis of the methodologies employed in the analysis of existing public opinion surveys, and to assist the PRISMS consortium by directing attention to gaps that need to be assessed by the Europe-wide survey that the PRISMS project will conduct in relation to these issues.

Chapter 6: Short comings & lessons learned

Iván Székely
Eötvös Károly Policy Institute

6 SHORTCOMINGS & LESSONS LEARNED

6.1 SUGGESTIONS TO INCLUDE NEW TYPES OF QUESTIONS IN THE PLANNED PRISMS SURVEY

Surveys in general, and surveys in the subject areas of privacy, security, surveillance and trust in particular, are designed to measure people's knowledge, opinion and attitudes in the investigated areas. The knowledge, opinion and attitudes are apparently dissimilar among individual respondents and respondent groups alike; the data may vary in similar surveys conducted in different time periods, or in the case of longitudinal research (where it is the temporal differences what researchers want to measure); and one can expect dissimilar results in surveys conducted in different samples of respondents, too. The latter case can be observed at sub-national level when different social or demographic groups are surveyed and at cross-national level when surveys extend to various countries, continents and cultural regions. (In exceptional cases exactly similar results can also be experienced but public opinion researchers and empirical sociologists basically presume that the surveyed population is not homogenous, and it is the differences themselves what they aspire to measure and explore.)

The distribution of data representing the knowledge, opinion and attitudes of the respondents can easily be presented with the help of simple descriptive statistics, but their characteristics and correlations can be further emphasized by various analysis techniques, from the creation of common variables, through cross-tables to multivariate statistical methodologies. For decision-makers who want to enact (or justify) regulatory measures on the basis of the results, or for service providers who want to develop marketing strategies based on these data, in many cases the simple distribution of data seems to be a sufficient point of reference, especially if it is presented in an attractive visual form. The media also prefers such descriptive statistics for presenting the (selected) results of a survey, thus emphasising or suggesting certain elements of the research findings. (Naturally, the possible biases and implicit favouritism, which have been mentioned in chapter 2 and 5, can be found in the presentation and interpretation of a simple set of data, too; however, complex analyses may further mask the inherent biases in the survey results.)

However, for researchers (and more demanding users of survey results) it is not only the measurable characteristics of the surveyed population that is of interest but also the factors, which may explain the differences at individual and group levels. In other words, the research question is not only "what" but also "why".

It is general practice that survey data are compared with demographic variables (e.g., age, gender etc.) and on this basis researchers try to show correlations, for example, between the degree of education on the one hand, and the knowledge, opinions and attitudes of the respondents in the given area on the other. Higher quality surveys may use the responses given to questions aimed at exploring attitudes, as explaining-segmenting factors, such as ideological or political preferences, which may have a significant role in the distribution of opinions. As a further possibility in large scale surveys, belonging to a cultural region is regarded as a segmenting factor (for example, Eastern and Western cultural hemispheres, or North-South differences), or countries as places of residence themselves are regarded as a composite factor in explaining differences in the distribution of survey data. Besides – if the nature of the research permits it –, questions borrowed from general social value surveys, such as the World Values Survey, can also be included in the survey questionnaires, thus the

distribution of responses to the core questions can be compared with the distribution of responses to these borrowed questions and consequently the supposed value preferences of the respondents. Chapter seven of the present deliverable provides an analysis of social value surveys, a typology of European countries with regard to their dominant value system, and points of reference for the countries where focus group discussions are to be conducted.

However, in the subject areas of the present research project – namely privacy, security, surveillance and trust – the above factors cannot explain entirely the differences in people's knowledge and opinion, nor their attitudes towards privacy and security. One can suppose a number of other factors, which may influence the opinion of the respondents, their knowledge in our subject areas, and their attitudes, which the above-listed analysis methods cannot explore. Therefore we suggest that the planned PRISMS survey, in addition to following the logic of earlier surveys, in order to ensure the comparability of the results, include some new questions, too, which go beyond the above mentioned explanations, and provide a new level of "explaining power", or at least may prove the suitability of such questions for exploring new correlations regarding the differences in people's opinion on, and attitudes towards, privacy and security.

We deem in particular the following areas of questions suitable for exploring these new correlations:

A. Personal life history

We presume that circumstances relating to the personal privacy of the respondents, especially in the early period of life, have a significant impact on how, in a later phase of their life, respondents will regard privacy and the competing interests and values. For example, responses to questions relating to:

- whether the respondent had a separate room during his childhood (alone or together with his brothers/sisters, if any),
- how many brothers and sisters he has,
- does he remember cases of secretly peeping into the life of other children, his parents or other adults; did these acts result in being detected, scolding and humiliation,
- did the schoolteachers catch the respondent's or his schoolmates' letters (paper or electronic) sent to his friends; if yes, was it publicly read,
- were private matters compulsory to discuss in a community (school class, family, friends), etc.
- may reveal important factors of the distribution of opinions in the given subject areas.

Certain stages of adult life history also belong to this group:

- housing (type of flat, separate rooms or shared rooms with others, living alone, in a small family or in a big family of several generations and relatives),
- workplace and work environment (for example, a long-range truck driver's work environment is very different from that of an administrative employee working in a large room, together with others),
- have these circumstances been intentionally chosen by the respondent, or accepted out of necessity.

We note here that such factors – similarly to the other questions detailed below – may have both positive and negative impact on people's demand for, and attitudes towards privacy.

B. Religious or philosophical beliefs

Information relating to somebody's religious or philosophical beliefs is a highly sensitive category of personal data, from both a legal and ethical points of view. Therefore it is less likely to include questions directly relating to such convictions of the respondent himself (and would probably result in a lower response rate): for example, whether he has such a belief, if yes, what kind of belief/religion/ it is, which church he belongs to, and whether he regularly practicing his duties originating from his religious conviction. Instead, we could ask respondents about their opinion on whether such factors have an impact on what people think about privacy, trust, security, or even surveillance. We suppose that the differences among the religions and churches regarding what is private and what is public, may influence the developing of the notion and value of privacy in the respondents' mind.

C. Belonging to minority groups

Belonging to one or more ethnic, religious, cultural, sexual or other minorities in society has certainly had an influence on what respondents think about the borderlines of private and public life. Similar to religion, belonging to a minority groups is highly sensitive information that respondents may not be willing to reveal, even if their details are kept anonymous . Here we could also ask the respondents' opinion in general about whether belonging to such groups – with examples – has a correlation with what people thing about their privacy. Alternatively, we could ask respondents whether they identify themselves with a minority group, without specifying the group.

D. Offline communication, social contacts

Recent surveys on people's opinion of privacy-related matters often include questions relating to the respondents' online communication habits, for example in their use of online social networks. However, questions relating to offline (personal) social contacts and communication may also reveal correlations with opinions and attitudes regarding privacy. Questions such as:

- what kind of social events do you participate in regularly,
- what kinds of information about you would you share with others (it is advisable to ask this question in a form of a list, or rather a matrix, e.g., list of information vs. list of communication partners),
- what would you be afraid of, or feel embarrassed, if your friends knew about you etc.

could shed light not only on the correlation of people's opinion on privacy and their personal communication habits, but also on the correlation between online and offline communication patterns.

E. Bad (and good) personal experience

Certain concrete, significant events can also have a lasting impact on the respondents' views on privacy and related areas. Questions relating to bad experience, such as ID theft, are not unique in surveys conducted in the subject areas of privacy and data protection. The planned PRISMS survey could also include such questions, with special regard to the large population it will investigate. We should not exclude positive experience either, since the successful, fair solving of a sensitive situation relating to privacy may also have a lasting impact on people's views.

F. Other sensitive personal data

Questions exploring other sensitive areas of the respondent's life, such as health status, pathological addictions, sexual preferences, criminal convictions etc., or rather asking the respondent's opinion on whether such circumstances in people's life may have an impact on how people think about privacy, can also explain some background factors in the distribution of survey data.

6.2 PRELIMINARY HYPOTHESES

With regard to the foregoing, we can formulate the following preliminary hypotheses, in addition to those presented in section 5:

(1) Characteristics of the respondents' personal life history have a significant correlation with the respondents' opinion on, and attitudes towards, privacy, security, trust and surveillance. This correlation is particularly strong in the case of circumstances and experiences in the early stages of the respondents' life (childhood, family life, school) but also traceable in adult age. Naturally, we expect to find correlations between certain demographic data and the circumstances of the respondents' personal life history (for example, higher income – more chance to have a separate room) but we believe that such demographic data cannot fully explain the opinions and attitudes of the respondents, with special regard to individual (bad and good) experience.

(2) The existence and characteristics of religious or philosophical beliefs (including the characteristics of the religion or church in question) show correlations with the respondents' opinion on, and attitudes towards, privacy, security, trust and surveillance.

(3) Belonging to ethnic, religious, cultural, sexual or other minorities in society also have a measurable impact on people's view on the borderlines of private and public life. Similarly, other sensitive personal data (health status, pathological addictions, sexual preferences, criminal convictions etc.) may also show correlations with the distribution of survey data. These correlations are bi-directional: belonging to a minority group, or having an illness do not necessarily result in a higher sensitivity to privacy.

(4) Not only online communication habits but also offline communication experience, including participation in social events, exchange of news and information, the nature of information shared with others, and the expectations of what should and what should not be divulged about the respondent's private life in the various social circles, show correlations with the respondents' views on privacy and related subject areas.

These hypotheses can be verified or refuted through formulating and asking the concerning questions in the survey, and through analysing the possible correlations between the answers. Naturally, we are aware that showing correlations is only the first step in explaining the distribution of data, or the factors influencing people's opinion and attitudes: the correlations need to be properly interpreted – and this belongs to a later phase of the research. We are also aware that the above enlisted questions are by far too much for including all of them in the questionnaire, given the practical and financial limitations of the survey. However, including some of these questions, which can be expected to have a strong explaining power, could significantly contribute to the exploration of the investigated subject areas. As in empirical research in general, here, too, the refuting of our hypotheses – in other words, proving that the above factors have no significant influence on the respondents' opinion on, and attitudes

towards privacy, security, trust and surveillance – would in itself enrich our knowledge on the subject areas of our planned survey.

Chapter 7: Analysis of social values surveys

Kerstin Goos and Michael Fridewald
Fraunhofer ISI

7 ANALYSIS OF SOCIAL VALUE SURVEYS

7.1 INTRODUCTION

As identified in the chapter one, the PRISMS project aims to understanding how citizens perceive the mutual relationship between security prospects on the one hand and privacy prospects on the other. In order to achieve this, as part of the multidisciplinary approach the project is following, a European wide survey will be conducted and profound insights into citizen's perceptions of privacy, security, trust and surveillance will be gained. The aim of this chapter follows a slightly different approach to previous chapters that focused on analysing existing public opinion surveys to instead, consider the potential disparities of the prospective respondents in relation to their cultural roots and thus focused our analysis on existing social value surveys. Accordingly, as will be highlighted in this chapter, we analysed European differences in terms of culturally related perceptions of privacy and security and related concepts.

Cultural values are central to understanding how privacy and security issues play out in public opinion surveys. It would be naive to conduct cross-national research without understanding how values shape people's perceptions and opinions on the subject in question. We assume that prevailing value orientations affect notions of privacy and security. Historical experiences, cultural heritages, the political system or the economic development shape the amount of interpersonal trust and trust in institutions within a society, the prevalence of value orientations such as individualism or deference to authority, and the extent to which fear of crime is an issue.

In order to achieve this, we draw upon analyses based on the following three social value surveys: the World Values Survey, the European Values Study and the European Social Survey. We choose these surveys because they are rather broad in their scope, particularly in terms of the amount of countries that are covered, as well as the issues that are covered. Furthermore, these surveys have been methodologically professionalised since they introduction in the 1980s.

For the purpose of investigating underlying factors that determine potential differences in perceptions of privacy, security and related concepts, we followed an exploratory approach. We drew on theoretical considerations about value theories and investigate existing cultural maps of Europe. As follows, as a first step the concept of values, definitions of values and an overview of value theories is given. Next, it is described how values can be measured and how the three investigated Social Value Surveys approach values. Subsequently, we outline European differences relating to values connected to privacy and security. As a final point we present a series of hypotheses to be considered in the construction of the PRISMS survey.

7.2 THE CONCEPT OF VALUES AND HOW VALUES CAN BE MEASURED

7.2.1 *The concept of values*

In general social scientists agree upon the idea that culture matters, though it is a contested question how culture matters and what kind of impact culture has on and within a society. Culture can be defined as a "rich complex of meanings, beliefs, practices, symbols, norms,

and values prevalent among people in a society."[494] The inevitable task of measuring culture, e.g., in order to compare different cultures, is obviously challenging. Scholars have been approaching this task by studying the system of law, by analysing the ways economic exchange is organised or by reviewing literature and art. However, such approaches follow an indirect approach and capture only part of a culture.[495] In contrast, values, or rather value priorities that are dominant in a society may be the most central feature of a culture[496] and reflect cultural conceptions of what is desirable. Thus, studying values is an appropriate approach to analysing culture.

Before going into detail about particular differences in value priorities and reasons for such variances within European countries or regions, we give a brief introduction to the research field of 'values'. As follows, the most common features of definitions of values are approached, and the historical development and relevance of values research are described. We also consider the measurement of values and the various methodological challenges.

Definition of "value"
Values are a multi-faceted concept and a vast amount of literature exists in relation to different approaches of how values can be defined (e.g., In 1976, Kmieciak conducted a literature review and came across 180 different value definitions within 400 publications dealing with values[497]). The term 'value' is an interdisciplinary term that is used in the diverse branches of the social sciences. Psychologists, economists, political scientists and sociologists apply the concept of values in their respective contexts. The concept of values is also used in many anthropological and philosophical studies. Since our aim is to develop differences in prevailing value orientations, the approach we are adopting is mostly a sociological one, however, due to the inherent fact that values guide the behaviour of individuals, the psychological facets of values do also play a role.

It is out of the scope of this report to fully elaborate all discussions about values and their definitions, or to summarise the literature in this field. Definitions or aspects of definitions are contested across groups of value researchers and a summary of the several definitions can hardly be achieved. Some approaches are very broad, some approaches are rather narrow and demarcation lines to cognate terms are divers. Instead of finding *the* ultimate definition, we will try to point out, as follows, the most common aspects of different definitions. By doing this, we are geared to the most well-known internationally active researchers dealing with values and value change, namely Schwartz, Inglehart and Hofstede, but we will also incorporate other prominent facets of values occurring in literature. The selection criteria are mostly based on practical and content related issues, since we will later focus on surveys that are conducted and developed by the aforementioned scholars.

The following conceptual definition of 'values', developed by Schwartz[498], summarises a couple of key features of values that are widely agreed upon in literature: A value is a "belief

[494] Schwartz, Shalom H., "A Theory of Cultural Value Orientations: Explication and Applications", in Yilmaz, Esmer and Thorleif Pettersson (eds.), *Measuring and Mapping Cultures: 25 Years of Comparative Value Surveys*, Brill, Leiden, 2007.
[495] Ibid.
[496] Weber, Max, "Die protestantische Ethik und der Geist des Kapitalismus", in *Gesammelte Aufsätze zur Religionssoziologie I [1920]*, Mohr, Tübingen, 1988; Schwartz, 2007.
[497] Kmieciak, Peter, *Wertstrukturen und Wertwandel in der Bundesrepublik Deutschland*, Otto Schwartz, Göttingen, 1976.
[498] Schwartz, Shalom H., "Are There Universal Aspects in the Structure and Contents of Human Values?", *Journal of Social Issues*, Vol. 50, No. 4, 1994, pp. 19-45.

pertaining to desirable end states or modes of conduct that transcends specific situations, guides selection or evaluation of behaviour, people, and events, and is ordered by importance relative to other values to form a system of value priorities"[499]. This definition leads to several main features of values, which will be described in detail as follows:

(1) Values are beliefs with *cognitive*, *affective*[500] and *behavioural* aspects[501]: (a) if a person has a value, he or she cognitively knows the correct way to behave (b) the affective element reflects the idea that a person can feel emotional about a value, and the (c) behavioural aspect exists in the sense that values in their function as an intervening variable lead to behaviour.
(2) Values are *not directly observable*[502], which poses several challenges for the measurement of values (see below).
(3) Values refer to *desirable goals*: the idea that values can be defined as "conceptions of the desirable which influence the selection from available modes, means, and ends of action"[503] is widely agreed upon[504]. At this point it is important to emphasise the difference between the *desired* (what people desire) and the *desirable* (what people ought to desire), especially in relation to the measurement of values. While usually social desirability is treated as something undesirable to the researcher since it creates biases, in the case of values it is perfectly respectable[505]. The two concepts are closely related, because desirability's are a subset of desires, "people can desire what they consider desirable, and label desirable things as desires". [506]
(4) A characteristic that distinguishes *values* from narrower concepts such as *norms* and *attitudes* is that they transcend specific actions and situations. Values are "enduring beliefs"[507] and can be activated in a variety of situations[508]; they are fundamental and changing slow. Furthermore it is assumed that values have a particular relevance for behaviour[509]. In contrast to that, attitudes are concepts that refer to specific actions, objects or situations, values are determinants of attitudes and attitudes are functions of values[510]. Norms also differ from values in several aspects: a norm is a prescription to behave in a specific way in a specific situation and they are external in a way that they

[499] Schwartz, Shalom H. and Wolfgang Bilsky, "Toward a theory of the universal structure and content of values: Extensions and cross-cultural replication", *Journal of Personality and Social Psychology*, Vol. 58, 1990, pp. 878-891.
[500] Schwartz, Shalom. H., "A Proposal for Measuring Value Orientations across Nations", Questionnaire Development Report of the European Social Survey, 2003.
[501] Rokeach, Milton, *The Nature of Human Values*, The Free Press, New York, 1973.
[502] McLaughlin, Barry, "Values in behavioral science", *Journal of Religion and Health*, Vol. 4, 1965, pp. 258-279.
[503] Kluckhohn, Clyde, "Values and value-orientations in the theory of action: An exploration in definition and classification", in Parsons, Talcott and Edward Shils (eds.), *Toward a general theory of action*, Harvard University Press, Cambridge, 1951.
[504] McLaughlin, 1965; Williams, Robin M., Jr., "Values", in Sills, David L (ed.), *International encyclopedia of the social sciences, Vol. 16*, Macmillan, New York, 1968. As stated above, many authors agree upon the approach of defining values as "conceptions of the desirable", but nevertheless, some authors also reject this view (see detailed discussion in van Deth, Jan W. and Elinor Scarbrough, "The Concept of Values", in van Deth, Jan W. and Elinor Scarbrough (eds.), *The Impact of Values*, Oxford University Press, Oxford, 1995.)
[505] Hofstede, Geert, *Culture's Consequences – Comparing Values, Behaviors, Institutions and Organizations Across Nations*, Sage, Thousand Oaks, London, Neu Delhi, 2001.
[506] van Deth and Scarbrough, 1995.
[507] Rokeach, 1973.
[508] Hofstede, 2001.
[509] van Deth and Scarbrough, 1995.
[510] Rokeach, 1973.

can be sanctioned from society. Norms are rather considered as means to achieve values. Moreover v*alue orientations* can be understood as internalised values.[511]

(5) All men, independent of their cultural background, possess the same values to different degrees. Cultures and the individuals belonging to a culture are characterised by their *value priorities*, i.e., the distinct value system that has been internalized.

(6) Values are organised in value systems. Relevant values that guide action have *relative importance*; internal conflicts between values are inherent. Trade-offs among the competing values is characteristic. Values are *ordered by importance* relative to one another, they are mutually related and form value systems with hierarchical structures.[512]

(7) Values have both *intensity* and *direction*[513]. The intensity of a value reflects the relevance that it has for an individual, the direction underpins that some outcomes are valued as bad and others as good. Values are not only reduced to morally desirable states, but also to morally questionable states.

(8) Values can be distinguished between end states and modes of conduct. In this vein, Rokeach differentiates terminal values (end states) from instrumental values (ways to get there). [514]

Values are often discussed in their function as a dependent variable, thus the impact of value orientations on social behaviour or political orientations. In addition, values can be treated as an independent variable, to ask what factors determine value orientations. Values as independent variables reflect the influences to which individuals and groups are exposed.

A first source of value orientations are needs or inborn temperaments.[515] "People evolve value priorities that cope simultaneously with their basic needs and with the opportunities and barriers, with the ideas of what is legitimate or forbidden, in their environment".[516] A second source is social experience, e.g., the social structure (education, age, gender, occupation, etc.) people adhere to as well as unique experiences (trauma, relation with parents, immigration, etc.) one makes shape value orientations.[517]

7.2.2 *Roots of values research*

Changes of value orientations that have happened asynchronous in different European countries have been identified as the main reason for current differences in predominant value systems. Thus, referring to theories of value change and having a closer look at modernisation theory is necessary in order to analyse differences in value priorities between countries.

Modernisation theorists generally agree on the assumption that the cultural, political and economic systems of a society refer to each other in a reciprocal relationship and that change in any of those systems is synchronous of change within other systems. The role culture plays within those complex interrelationships within a society are various and reflect the traditions of different scientific schools. Two schools dominated the theory of modernisation for a long time: On the one hand the Marxist approach, which states that the economic system mostly

[511] Welzel, Christian, "Werte und Wertewandelforschung", in Kaina, Viktoria and Andrea Römmele (eds.), *Politische Soziologie. Ein Studienhandbuch*, VS Verlag für Sozialwissenschaften, Wiesbaden, 2009.
[512] Hofstede, 2001.
[513] Ibid.
[514] Rokeach, 1973.
[515] Ibid.
[516] Schwartz, "A Proposal for Measuring Value Orientations across Nations", 2003.
[517] Ibid.

influences the political and the cultural system of a society. Marx underlined the economic determinism by arguing that technological progress determines the economic system, which in turn influences the cultural and political system. Once industrialisation begins, pervasive social and cultural consequences arise. The second approach is based on Weber's assumptions that the cultural system shapes the economic and political life. He mainly derived his approach from his early work where he researched on the relation between the capitalist economy and the Puritan determination to work.[518] Weber supports the idea that cultural beliefs have the capability to influence the economic and political system. Durkheim follows a similar rationale. Both focus on the role of norms and values for social life, although Weber and Durkheim pursue different sociological ideas, Weber the functionalistic systems theory, Durkheim the institutionalist theory of action. Within the theory of action it is assumed that values guide behaviour. Durkheim took up the position that collective values, organised in a normative system, guarantee the stability of social organisations.

An influential researcher in the field of values research is Talcott Parsons, who revaluated values in his theory of action. Parsons' structural functionalist approach represents an advancement of his theory of action where values play a crucial role, since they are the core aspect of culture and are constitutional for the survival of societies.

From a historical-sociological view, in the fifties and sixties the tendency evolved that the structural functionalist approach could be a dominant one. But such predictions did not come true, instead a paradigmatic change occurred and sociology instead focused on the methodological individualism.[519] Approaches rooting in this theoretical line assume that it is not culture that guide's action, but the maximisation of individual benefits. Nevertheless some theorists continued to focus on values research, which finally experienced its breakthrough in the seventies due to the emergence of an empirical branch of values research. With the advent of comparative values research, pushed by researchers such as Rokeach, Inglehart, and Klages, to name the most prominent ones, the empirical data basis for extensive research and the analysis of changes of priorities in value orientations was set.

7.2.3 *Contemporary values research*

Meanwhile, mainly resulting from analyses based on comparative value surveys, the theory of value change gained a quite dominant position within values research. This theoretical approach is based on complex circular processes between macro level circumstances, individual orientations and individual behaviour.[520] Since it is assumed that values have orientation and life guiding functions, prevailing values are closely linked to life experiences one has made. Thus, if the environment changes, value orientations are also under pressure to change. Underlying dynamics of change on the macro-level could result from technological development or economic growth. Changes such as the spread of affluence, on-going division of labour, decline of the agricultural sector, urbanisation, rising levels of education, increasing mobility or growth of the mass media influence individual values. Value differentiation in terms of intergenerational value differences typically occurs as a result of tensions between tendencies of value persistence and pressure to change. It is no longer contested within the

[518] Weber, 1988.
[519] Hillmann, Karl-Heinz, "Zur Wertewandelforschung: Einführung, Übersicht und Ausblick", in Oesterdiekhoff, Georg W. and Norbert Jegelka (eds.), *Werte und Wertewandel in westlichen Gesellschaften, Resultate und Perspektiven der Sozialwissenschaften*, Leske + Budrich, Opladen, 2001.
[520] van Deth and Scarbrough, 1995.

values research community that a value change has taken place since the sixties; nevertheless in relation to specific aspects of the value change various positions exist.

Ronald Inglehart: Theory of value change

The best-known contemporary work in this vein is the "silent revolution" by Inglehart[521], who dominates the international debate about value change within the social sciences. Inspired by Abraham Maslow's pyramid of needs[522], Inglehart developed the core idea of the theory, namely that value change comes along with a shift from materialist to post- materialist values. Central to his approach are two underlying hypotheses: the "scarcity hypothesis" and the "socialisation hypothesis". The first hypothesis refers to the idea that the greatest subjective value priorities stem from those things that are in relatively short supply. The second hypothesis assumes that basic value orientations of an individual reflect the conditions prevailing during one's pre-adult years. Inglehart connects economic security with personal value orientations, which means that value priorities of an individual depend on the economic circumstances under which someone has grown up. As long as basic human needs are not met, materialist values prevail; as soon as material needs are satisfied, post-materialist values can unfold. Hence, with the growing prosperity of a society, the pursuit of post- materialist values increases due to the satisfaction of survival needs.

Helmut Klages: Theory of value synthesis

A second theory of value change is the value synthesis approach, which has been deliberately developed by Klages in order to contrast the materialist/post-materialist approach of Inglehart.[523] Klages conceives value change as being reflected in differences in the proliferation of types of values. Dependent on someones aims in life (e.g., participative, conformist, expressive, hedonist, altruistic aims), individuals can be assigned to one of the following groups: conventionalists, idealists, people who resigned (the "resigned"), and active realists. While beliefs of conventionalists and idealists are rather similar to the two hybrid types, materialism and post-materialism, the "resigned" and the active realists, offer new aspects. The "resigned" rate a lot of values low and the active realists rate a lot of values high. Those active realists reflect the value synthesis, i.e., the idea that traditional and modern values need not be contrary or mutually exclude each other, but can also be interdependent.

Shalom H. Schwartz: Schwartz value circle

Schwartz developed a 'theory of Cultural Value Orientations', which assumes that "cultural value orientations evolve as societies confront basic issues or problems in regulating human activity".[524] The values he derived for his cultural theory are based on three issues that confront all societies:

1. The nature of the relations or the boundaries between the person and the group is reflected by the cultural dimension autonomy vs. embeddedness.
2. The dimension egalitarianisms vs. hierarchy reflects the problem of how it is guaranteed that people behave in a responsible manner that preserves the social fabric.

---

[521] Inglehart, Ronald, *The Silent Revolution: Changing Values and Political Styles among Western Publics*, Princeton University Press, Princeton, 1977; Inglehart, Ronald, *Modernisierung und Postmodernisierung. Kultureller, wirtschaftlicher und politischer Wandel in 43 Gesellschaften*, Campus, Frankfurt/Main, 1998.

[522] Maslow, Abraham, *Motivation and personality*, Harper & Row, New York, 1954.

[523] Klages, Helmut and Willi Herbert, *Wertorientierung und Staatsbezug: Untersuchungen zur politischen Kultur in der Bundesrepublik Deutschland*, Campus, Frankfurt, New York, 1983; Klages, Helmut, *Wertedynamik: Über die Wandelbarkeit des Selbstverständlichen*, Fromm, Zürich, Osnabrück, 1988.

[524] Schwartz, "A Theory of Cultural Value Orientations: Explication and Applications", 2007.

3. The third bipolar dimension of culture is labelled harmony vs. mastery and takes up the problem of regulating how people manage their relations to the natural and social world.

One approach that Schwartz takes in order to empirically evaluate his theory is to "infer the cultural value orientations that characterize societies by averaging the value priorities of individuals in matched samples from each society"[525]. To achieve this, as a first step he theoretically conceptualised values.

Schwartz proposes to distinguish values according to the type of motivational goals a value expresses. He assumes that the "basic human values likely to be found in all cultures are those that represent universal requirements of human existence (biological needs, requisites of coordinated social interaction, and demands of groups functioning) as conscious goals." Drawing on previously identified values by other researchers and religious and philosophical writings, Schwartz aimed to develop a set of universal values that could be used for interpersonal and intercultural comparisons.[526] He suggested ten basic values: universalism, benevolence, conformity, tradition, security, power, achievement, hedonism, stimulation and self-direction (see figure 43 below). Schwartz assumes that values which are directly neighboured are compatible, while values which are positioned rather far away from each other are conflicting values. Those conflicts between values are illustrated through the two dimensions openness to change vs. conservation and self-enhancement vs. self-transcendence. Schwartz used the 'Schwartz Value Inventory' (see below) to test his considerations and discovered that the items are understood in a similar way within a huge number of different countries.

Figure 43: Schwartz value circle[527]

7.2.4 *The measurement of values*

By accepting the idea that individual persons may not directly access values, several approaches to indirectly measure values have been developed (Table 19): Indirect inferences can be made from nonverbal behaviour, either from provoked or natural deeds. Provoked deeds can be assessed through laboratory experiments or field experiments, which are lacking

[525] Ibid.
[526] Smith, Peter B. and Shalom H. Schwartz, "Values", in Berry, John W., et al. (eds.), *Handbook of Cross-Cultural Psychology, Vol. 3, Social Behaviour and Applications*, Allyn and Bacon, Needham Heights, 1997; Schwartz, "A Theory of Cultural Value Orientations: Explication and Applications", 2007.
[527] Ibid., p. 87.

"natural conditions". Those natural conditions can be achieved through the direct observation of natural behaviour, which is, a methodologically challenging task. Additionally, a differentiation between natural and provoked words can be made: the measurement of words in a natural, not provoked manner could be derived from a discourse analysis of cultural products like movies or literature; capturing values through provoked words means surveying people to receive responses to questions that reflect underlying values. The method that is most often used in order to capture values is the conducting of questionnaires, i.e., the collection of provoked words. While in early studies of values the means to measure them were interviews, essays or open-ended questions, contemporary research has concentrated on structured questionnaires.[528]

Table 19: Approaches to measure values[529]

	Provoked	**Natural**
Words	Interviews Questionnaires Projective Tests	Content analysis Discussions Documents
Deeds	Laboratory experiments Field experiments	Direct observation Use of available descriptive statistics

In general, nowadays the use of standardised questionnaires is a widely applied method to conducting values research, nevertheless, different approaches exist in relation to the operationalisation of values. Different researchers argue for various methods in order to infer value orientations from survey responses. For instance, Bales and Couch[530] collected nearly 900 different formulations of values. They took those as a start and then reduced them to four clusters: authority, self-restraint, equality and individuality. Those four clusters are the result of work with a test population of 500 U.S. students. Musek[531] followed a similar approach and reduced 54 values to four clusters: hedonism (pleasure), potency (achievement), moral (duties) and fulfilment (self-actualization).

Hofstede, Inglehart and Schwartz have done influential work in developing the most basic value dimensions for comparative values research. This is also due to intensive theoretical considerations that accompany their work. Inglehart and Schwartz are furthermore more or less directly involved in the World Values Survey, the European Values Study and the European Social Survey, which produces huge data sets that are available for individual research. Accordingly, the approaches of those scholars will now be explained in greater detail.

Shalom H. Schwartz

As most researchers do, Schwartz also followed the tradition of Rokeach to ask about basic values directly in questionnaires.[532] The Rokeach Value Survey (RVS) is a well-known and influential instrument developed by Milton Rokeach in the early 1970s. The questionnaire

[528] Smith and Schwartz, 1997.
[529] Hofstede, 2001.
[530] Bales, Robert. F. and Arthur. S. Couch, "The value profile: A factor analytic study of value statements", *Sociological Inquiry*, Vol. 39, 1969, pp. 3-17.
[531] Musek, Janek, "The universe of human values: A structural and developmental hierarchy", *Studia Psychologica*, Vol. 35, 1993, pp. 321-326.
[532] Smith and Schwartz, 1997.

consists of two lists, one with 18 instrumental values and one with 18 terminal values and the respondents are asked to rank the values in the respective list.[533]

Inspired by Rokeach's approach, Schwartz used the RVS as a starting point and developed a new theory and methodology for studying values. He derived groups of values according to the motivational goal a value expresses. Theoretically driven, he used existing literature about cultural differences to group values in ten motivationally distinct types of values: power, achievement, hedonism, stimulation, self-direction, universalism, benevolence, tradition, conformity, and security.[534] Schwartz developed a questionnaire, the 'Schwartz Value Survey' with 56 questions representing the different groups of values.[535] In this survey, the respondents are asked to rate the importance of the 56 values as "guiding principles in your life". The questionnaire was conducted in 54 different countries, with samples usually consisting of urban school teachers and college students. The focus lay on teachers because it is assumed that they play a key role in value socialisation. Schwartz analysed the data he gained and concluded that his theoretically derived dimensions (change vs. conservation and self-enhancement vs. self-transcendence) were found in almost every sample.

As an alternative to, and advancement of the Schwartz Value Survey, Schwartz developed the 'Portrait Values Questionnaire' (PVQ). In order to avoid a dominance of Western values, Schwartz developed the questionnaire in cooperation with international researchers. The PVQ was based on the same theoretical approach, but uses a different method. Instead of rating the importance of values, short verbal portraits of different people are given and the respondent is asked to decide "How much like you is this person?", and chooses out of a range from "very much like me" to "not like me at all". The original version of the PVQ consists of 40 items. This was condensed in the European Social Survey to a selection of 21 items , which was then called the Human Value Scale.[536]

Geert Hofstede

Hofstede's approach to measuring cultural values is based on the IBM international employee attitude survey program, which was led by Hofstede and conducted between 1967 and 1972. He developed the questions by using data derived from questionnaires originally designed for audits of company morale. He identified four value dimensions: power distance, collectivism – individualism, masculinity – femininity and uncertainty avoidance.[537]

1. Power distance: this index reflects the tolerance of cultures in relation to power inequality and acceptance of centralised power.
2. Individualism – collectivism: cultures can be distinguished in relation to collectivist and individualist values.
3. Masculinity – femininity: this dimension reflects the gender equality tolerance.
4. Uncertainty avoidance: high uncertainty avoidance scores reflect a high resistance to change.

[533] Rokeach, 1973.

[534] Smith and Schwartz, 1997; Schwartz, "A Theory of Cultural Value Orientations: Explication and Applications", 2007.

[536] Schwartz, "A Proposal for Measuring Value Orientations across Nations", 2003. See Annex 2, where all items of the Human Values Scale are listed.

[537] Zureik, Elia, Lynda Harling Stalker and Emily Smith, "Background Paper for the Globalization of Personal Data Project International Survey on Privacy and Surveillance", The Globalization of Personal Data Project, Queen's University, Kingston, Ontario, 2006.

In order to avoid Western ethnocentrism, the Chinese Value Survey (CVS) was developed by Chinese researchers, analogous to Hofstede's questionnaire. An analysis of the questionnaires, answered by Chinese students, resulted in the same four dimensions plus a fifth dimension, called 'Long-Term Orientation'.[538]

Ronald Inglehart
A core concept of Inglehart's approach is the intergenerational shift from materialist to post-materialist value priorities. This is indeed only one component of the theory of post modernisation, but one that is captured quite well. The wording of the questions that are used to measure this dimension is the following:

> "People sometimes talk about what the aims of this country should be for the next ten years. On this card are listed some of the goals which different people would give top priority. Would you please say which one of these you, yourself, consider the most important? And which one would be the next most important?"[539]

In order to facilitate responding response, the items are separated into three item batteries, and each of the batteries comprises two materialist aims and two post- materialist aims. In addition, the World Values Survey questionnaire consists of a large amount of items that reflect emphasis on survival values, self-expression values, traditional and secular-rational values.

Similarities of value taxonomies
Although the approach of measuring values as well as the theoretical considerations of the respective researchers is different, some similarities between prevailing value orientations can be identified.[540] The traditional/secular-rational dimension developed by Inglehart broaches issues of authority. Traditional societies are societies where traditional values such as obedience or male dominance are dominant, and absolute standards of morality prevail. This conception overlaps with the autonomy/embeddedness dimension of Schwartz, since both dimensions tackle the degree to which the individual is submerged in all-encompassing structures of tight mutual obligations. Core aspects of embeddedness are the strong ties between the individual and religious and national or family groups which give life a meaning. The concept of autonomy focuses on the weakening of encompassing structures that frees individuals to think, do, and feel more independently. In secular-rational societies the emphasis lies on similar ideas. Conceptual overlaps between Inglehart's traditional/secular-rational dimension and Schwartz' autonomy/embeddedness dimension exist. Nevertheless, by examining correlations between the dimensions, it is revealed that the two dimensions apparently encompass slightly different aspects of culture, which could be explained by the centrality of religion in Inglehart's index.

Further conceptual overlaps exist between the traditional/secular-rational dimension and the egalitarianism/hierarchy dimension. Both dimensions concern deference to authority. Empirical associations confirm that further overlaps are rather low. A rather unexpected empirical correlation was found between the traditional/secular-rational dimension and the harmony/mastery dimension. Schwartz finds an explanation in the idea that "more secular-

[538] Hofstede, Geert and Gert Jan Hofstede, *Lokales Denken, globales Handeln. Interkulturelle Zusammenarbeit und globales Management*, Deutscher Taschenbuch Verlag, München, 2009.
[539] Root version of the WVS 2005 questionnaire.
http://www.worldvaluessurvey.org/wvs/articles/folder_published/survey_2005/files/WVSQuest_RootVers.pdf
[540] Schwartz, "A Theory of Cultural Value Orientations: Explication and Applications", 2007.

rational societies are also societies that tend more to emphasise fitting into the natural and social world as it is, trying to understand and appreciate rather than to change or to exploit".[541] In relation to the second dimension developed by Inglehart, the survival/self-expression dimension, similarities exist with the autonomy/embeddedness dimension. Conceptually, those two dimensions overlap insofar as both "concern the degree to which individuals should be encouraged to express their uniqueness and independence in thought, action and feelings."[542] Correlations between the dimensions confirmed these assumptions empirically.

A similar picture is given for correlations between Inglehart's survival/self-expression dimension and Schwartz' egalitarianism/hierarchy dimension. The assumption that parallels exist between the degree of egalitarianisms and the degree of trust, tolerance and support of equal rights of out-groups, is empirically confirmed. According to Schwartz those overlaps "strongly support […] the idea that these dimensions capture real, robust aspects of cultural difference".[543]

7.2.5 *Methodological considerations*

Since values are rather complex constructs, debates about methodological considerations and the measurement of values are controversial.

One challenge that has been contested since methods of value measurement have been developed is the question if *ranking* or *rating* instruments are more appropriate in order to capture value orientations. This question is highly relevant to the theoretical approach that is followed by the respective researchers (see above).

In order to avoid the problem of response bias, it has been suggested to use rankings. Response biases could arise, since respondents with different cultural backgrounds vary in the way they typically respond to rating scales.[544] It seems to be a challenge for researchers to identify if response differences reflect differences in value orientations or if this has to be ascribed to differences in relation to rating scale formats. Different procedures to correct response biases have been suggested.[545] On the other hand, other researchers find arguments against ranking. Critics of the ranking method assume that ranking forces respondents to make statements they otherwise wouldn't make.[546] Due to a forced choice situation, a biased portrait of values may be given.

A further challenge is posed by the problem of *meaning equivalence.* An indispensable prerequisite for comparative values research is the appropriate translations of the wording of the survey, in order to be able to exclude biases resulting from wrong translations. But still,

---

[541] Ibid.
[542] Ibid.
[543] Ibid.
[544] Smith and Schwartz, 1997.
[545] van de Vijver, Fons J. R. and Kwok Leung, "Methods and data analysis of comparative research", in Berry, John W., et al. (eds.), *Handbook of Cross-Cultural Psychology, Vol. 1, Theory and Method*, Allyn and Bacon, Needham Heights, 1997.
[546] Klages, Helmut, "Die gegenwärtige Situation der Wert- und Wertewandelsforschung - Probleme und Perspektiven", in Klages, Helmut, et al. (eds.), *Werte und Wandel*, Campus, Frankfurt/Main, 1992; Bürklin, Wilhelm, Markus Klein and Achim Ruß, "Dimensionen des Wertewandels: eine empirische Längsschnittanalyse zur Dimensionalität und der Wandlungsdynamik gesellschaftlicher Wertorientierungen", *Politische Vierteljahresschrift*, Vol. 35, No. 4, 1994, pp. 579- 606.

even the best translations cannot exclude the possibility of different meanings of value expressions across Europe. The content validity (representativeness of the results between different samples) is necessarily low. It seems to be a questionable practice to use instruments that were developed in one country in another cultural environment.[547] Several possible solutions to the problem of meaning equivalence have been developed, e.g., some researchers investigate if the structure of relations among the values they study is similar within each culture. It is assumed that if values have similar meanings across cultures, the inter-correlations among these values should be similar as well.

In terms of interpretation of the results of value surveys, it has to be made clear that a difference exists in relation to whether measurements are based on self-descriptions or on ideological statements. The first approach captures values as the desired and implies that words such as important/unimportant are used, the latter captures values as the desirable, and words such as agree/disagree are used.[548]

7.3 MAPPING EUROPEAN VALUES

7.3.1 *Social value surveys*

As discussed above, several approaches to measuring values and to conduct cross-national values research exist. Meanwhile unique databases based on cross-national surveys have also been developed. This vast amount of comparative data sets in order to research values and value change has been enabled due to the prospering cross-national values research that has been flourishing since the seventies.

In the tradition of quantitative variable oriented approaches, where generality is given preference over complexity[549], we analyse the survey results in an exploratory manner. The surveys that are used in order to detect differences in value orientations between different European countries or groups of European countries are the World Values Survey, the European Values Study and the European Social Survey. These three surveys have been chosen due to their broadness in relation to the range of values and the coverage of nations that they cover.

European Values Study
"The European Values Study is a large-scale, cross-national, and longitudinal survey research program on basic human values."[550] Its roots can be traced back to the European Values Systems Study Group (EVSSG), which was initiated in the late seventies by Jan Kerkhofs from the Catholic University of Leuven and Ruud de Moor from Tilburg.[551] The main interest of the study group was to develop value patterns of West European countries and to explore a potential existence and the extent of a value change. The questionnaire covers orientations in life spheres such as politics, socio-economic life, religion, morality, family, marriage, sexuality, work and leisure time.

---

[547] Hofstede, 2001.
[548] Ibid.
[549] Ragin, Charles C., *The Comparative Method*, University of California Press, Berkeley, 1987.
[550] http://www.europeanvaluesstudy.eu/evs/about-evs/
[551] See further information: Arts, Wilhelmus Antonius and Loek Halman, "European Values at the Turn of the Millennium: An Introduction", in Arts, Wilhelmus Antonius and Loek Halman (eds.), *European Values at the Turn of the Millennium*, Brill, Leiden, Boston, 2004.

The first wave was conducted in 1981. At that time, the countries were selected based on the pragmatic criteria of the availability of funding. After the project attracted worldwide attention, a further survey was prepared and conducted between 1990-91. The aim behind the continuation of the European Values Study was to monitor value changes and compare differences in value orientations between European regions. Further waves were carried out in 1999/2000 and 2008; meanwhile each European country has been participating in at least one wave.

Table 20: European Values Study[552]

Wave	Years	Countries/Regions	Respondents
1	1981-1984	16	19,378
2	1990-1993	29	38,213
3	1999-2001	33	41,125
4	2008-2010	47	67,786
Longitudinal data file 1981-2008		49	166,502

World Values Survey

The initiator of the World Values Survey (WVS) was Ronald Inglehart from the University of Michigan. The EVS, which can be called the "cradle of the WVS", caught his interest and made him put every effort into getting the EVS survey done in other countries than those participating in the EVS. The first World Values Survey in 1981 was a replication of the European Values Study and expanded the covered countries in Europe with 14 non-European countries. As a result, profound insights into value changes have been gained, and in order to monitor these changes and probe more deeply into their causes and consequences, additional waves were carried out in 1995, 2000, 2005 and 2010. From 1995 onwards, special attention was given to better coverage of Non-Western societies. The topics covered in the World Values Survey included: life satisfaction, health, education, trust, participation, employment, science and technology, politics and democracy or government responsibilities.

The mission statement of the World Values Survey is to "help scientists and policy-makers better understand worldviews and changes that are taking place in the beliefs, values and motivations of people throughout the world."[553] Currently, worldwide networks of researchers are involved in carrying out the project, and each country has its own principle investigator, who is in charge of the survey in the respective country. The key idea of this network of social scientists is that in exchange for collecting data in the respective country, each participant gets access to the data from all the other participating countries. Usually each survey is dependent on local funding.

Table 21: World Values Survey[554]

Wave	Years	Countries	Population	Respondents
1	1981-1984	20	4,700,000,000	25,000
2	1989-1993	42	5,300,000,000	61,000
3	1994-1998	52	5,700,000,000	75,000

[552] European Values Survey, "Participating countries and country-information", 1981–1999, http://www.europeanvaluesstudy.eu/evs/surveys/; EVS, Integrated Dataset (EVS 2008), 2011; EVS Longitudinal Data File (1981-2008), 2011.
[553] http://www.worldvaluessurvey.org/
[554] http://www.worldvaluessurvey.org/

Wave	Years	Countries	Population	Respondents
4	1999-2004	67	6,100,000,000	96,000
5	2005-2008	54	6,700,000,000	77,000
Four-wave aggregate data file		80		257.000

European Social Survey

The European Social Survey (ESS) is an academically driven social survey that aims to monitor "changing public attitudes and values within Europe" and at investigating those attitudes and values in relation to changing institutions.[555] A further goal of the founder Roger Jowell and supporters of the ESS is to "advance and consolidate improved methods of cross-national survey measurement in Europe and beyond".[556] The organisational structure contains a Specialist Advisory Groups (Question Design Teams, Methods Group, Sampling Panel and Translation Taskforce), a Scientific Advisory Board, a Central Coordinating Team, the Funders' Forum and National Coordinators and Survey Institutes. The first wave of studies took place in 2002/2003 and the latest round in 2010/2011. Meanwhile the ESS covers 30 nations to reveal profound insights into long-term changes in public orientations in Europe.[557] The ESS is funded through the Framework Programmes of the European Commission, the European Science Foundation and several national funding bodies. The biannual questionnaires consist of several core modules that cover media, social trust, politics, the Human Value Scale, and a couple of rotating modules. The rotating modules are chosen in an open competition between transnational teams and have covered the following topics: immigration and asylum issues and citizen involvement (2002), health and care seeking and economic morality (2004), timing of life and personal and social wellbeing (2006), welfare and ageism and trust in the police and courts (2008).

Table 22: European Social Survey[558]

Wave	Years	Countries	Overall case count
1	2002/2003	22	42,359
2	2004/2005	26	47,537
3	2006/2007	25	43,000
4	2008/2009	30	56,752
5	2010/2011	26	50,781

7.3.2 *The cultural diversity of Europe*

As identified in this chapter, values are multi-faceted, not observable conceptions of the desirable. Individuals inherently possess value systems, in which values are subjectively ordered depending on value priorities. Aggregations of surveyed value priorities of individuals reveal that different value priorities prevail in different European societies. Values can be analysed from a micro- and macro perspective. The micro perspective plays a role insofar as that the personality of an individual is shaped by value orientations.[559] From a macro perspective, values shape societies culturally. Hofstede, Inglehart and Schwartz infer value orientations that characterize societies by averaging value priorities of individuals in matched samples from each society.[560]

[555] http://www.europeansocialsurvey.org/
[556] http://www.europeansocialsurvey.org/
[557] Arts and Halman, 2004.
[558] European Social Survey, ESS Documentation Reports (5 volumes), 2012.
[559] Allport, Gordon W., *Personality. A psychological interpretation*, Holt, New York, 1937.
[560] Schwartz, "A Theory of Cultural Value Orientations: Explication and Applications", 2007.

The approach we follow in the remainder of this chapter is an exploratory one. By examining the existing literature and empirical analyses in relation to differences in underlying value orientations across Europe, the relevant values surrounding privacy and security are captured. A vast amount of literature on value change and value research exists, and a lot of different value orientations have been studied intensely. However, whilst some value orientations such as materialism, post-materialism, religiosity, feminism and ecologism are well studied, others that are not covered by one of the three big surveys analysed here , are rather difficult to grasp. This also accounts for values relevant to the context of PRISMS. Direct references to privacy do not exist and security is only partly directly covered. Thus, besides analysing the direct references, indirect references such as personal autonomy and individualism are drawn upon. Focus here, will be on the mapping of values derived from the EVS, the WVS and the ESS.

World Values Map

The theory of value change is based on empirical data gained from the WVS. Hence, in contrast to the approach of Schwartz who developed a value scale based on theoretical considerations, Inglehart derived the theory of value change empirically driven. In order to illustrate the findings in relation to differences and similarities according to the people's value priorities, the World Values Map has been developed.

For the construction of the World Values Map the survey results are plotted in a two dimensional space consisting of the survival/self-expression dimension and the traditional/secular-rational dimension as the two axes. According to Inglehart, these two dimensions are the key dimensions of cross-cultural variation.[561] The first dimension reflects a continuum between emphasis on economic and physical security and an emphasis on self-expression, subjective well-being and quality of life concerns. The second dimension reflects a continuum between religious and traditional values and secular, bureaucratic and rational values. The researchers tested the robustness of the two dimensions throughout the survey waves between 1990 and 2000 and came to the conclusion that they are robust over time despite varying numbers of participating countries. They furthermore claim that those two dimensions explain more than 70% of cross-national variance.

The underlying indicators of traditional value orientations are an emphasis of the importance of religion, a strong sense of national pride, the rejection of abortion, divorce, suicide; the idea that children should rather learn obedience and religious faith than independence and determination and more respect for authority. Secular-rational values emphasise the opposite, i.e., the emphasis lies on freedom and individual moral choices, high tolerance for other opinions and beliefs.

Survival values emphasise a priority to economic and physical security over self-expression and quality of life, a self-description of not being very happy, the absence of justifiability of homosexuality, reluctance to sign petitions and low level of interpersonal trust. The emphasis lies on materialist orientations and traditional gender roles. Again, self-expression values emphasise the opposite; people tend to value individual freedom and are more critical toward actual democratic performance.

[561] Inglehart, Ronald, "Mapping Global Values", in Esmer, Yilmaz and Thorleif Pettersson (eds.), *Measuring and Mapping Cultures: 25 Years of Comparative Value Surveys*, Brill, Leiden, Boston, 2007.

According to Inglehart, the following tables show those variables which are relatively strongly linked with the respective dimension:

Table 23: Correlates of traditional vs. secular-rational values[562]

Traditional values emphasise the following	**Correlation with traditional/secular-rational values**
Religion is very important in respondent's life	0,89
Respondent believes in Heaven	0,88
One of respondent's main goals in life has been to make his/her parents proud	0,81
Respondent believes in Hell	0,76
Respondent attends church regularly	0,75
Respondent has a great deal of confidence in the country's churches	0,72
Respondent gets comfort and strength from religion	0,71
Respondent describes self as "a religious person"	0,66
Euthanasia is never justifiable	0,65
Work is very important in respondent's life	0,63
There should be stricter limits on selling foreign goods here	0,61
Suicide is never justifiable	0,60
Parents' duty is to do their best for their children even at the expense of their own well-being	0,57
Respondent seldom or never discusses politics	0,57
Respondent places self on Right side of a Left-Right scale	0,57
Divorce is never justifiable	0,56
There are absolutely clear guidelines about good and evil	0,56
Expressing one's own preferences clearly is more important than understanding others' preferences	0,56
My country's environmental problems can be solved without any international agreements to handle them	0,53
If a woman earns more than her husband, it's almost certain to cause problems	0,49
One must always love and respect one's parents regardless of their behaviour	0,45
Family is very important in respondent's life	0,43
Relatively favourable to having the army rule the country	0,41
R. favors having a relatively large number of children	0,40
(Secular-rational values emphasise the opposite)	
The number in the right hand column shows how strongly each variable is correlated with the traditional/secular-rational values index. The original polarities vary; the above statements show how each item relates to the traditional/secular-rational values index.	

[562] Ibid.

Table 24: Correlates of survival vs. self-expression values[563]

Survival values emphasise the following	**Correlation with survival/self-expression values**
Men make better political leaders than women	0,86
Respondent is dissatisfied with financial situation of his/her household	0,83
A woman has to have children in order to be fulfilled	0,83
R. rejects foreigners, homosexuals and people with AIDS as neighbours	0,81
R. favors more emphasis on the development of technology	0,78
R. has not recycled things to protect the environment	0,78
R. has not attended a meeting or signed a petition to protect the environment	0,75
When seeking a job, a good income and safe job are more important than a feeling of accomplishment and working with people you like	0,74
R. is relatively favourable to state ownership of business and industry	0,74
A child needs a home with both a father and a mother to grow up happily	0,73
R. does not describe own health as very good	0,73
One must always love and respect one's parents regardless of their behaviour	0,71
When jobs are scarce, men have more right to a job than women	0,69
Prostitution is never justifiable	0,69
Government should take more responsibility to ensure that everyone is provided for	0,68
R. does not have much free choice or control over his/her life	0,67
A university education is more important for a boy than for a girl	0,67
R. does not favour less emphasis on money and material possessions	0,66
R. rejects people with criminal records as neighbours	0,66
R. rejects heavy drinkers as neighbours	0,65
Hard work is one of the most important things to teach a child	0,62
Tolerance and respect for others are not the most important things to teach a child	0,62
Scientific discoveries will help, rather than harm, humanity	0,60
Leisure is not very important in life	0,60
Friends are not very important in life	0,58
Having a strong leader who does not have to bother with parliament and elections would be a good form of government	0,56
R. has not and would not take part in a boycott	0,56
Government ownership of business and industry should be increased	0,55
Democracy is not necessarily the best form of government	0,45
R. opposes sending economic aid to poorer countries	0,42
(Self-expression values emphasise the opposite)	
The number in the right hand column shows how strongly each variable is correlated with the survival/self-expression values index. The original polarities vary; the above statements show how each item relates to the survival/self-expression values index.	

[563] Ibid.

Based on data from the 2005 wave, a two-dimensional cultural map (Figure 44) has been developed, where all participating countries are located in relation to the responses of the people surveyed in the respective country.

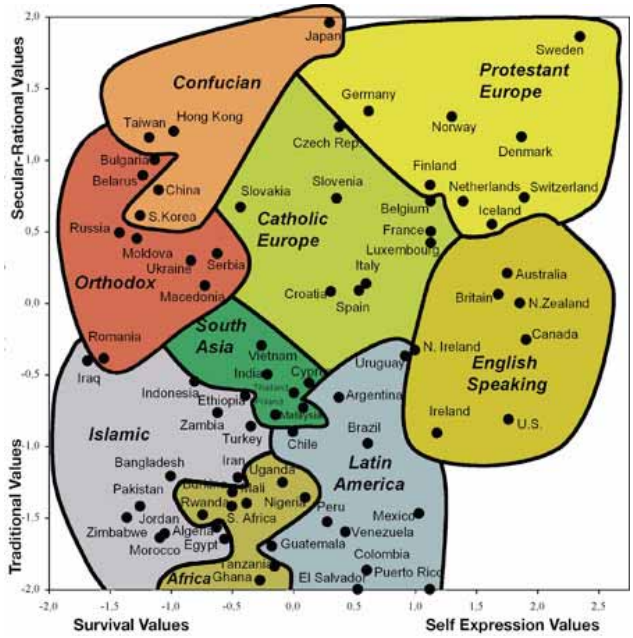


Figure 44: World values survey[564]

The map shows cultural zones in which similar countries are grouped together. These are South Asia, Africa, Latin America, english speaking countries, protestant Europe, confucian societies, ex-communist societies and catholic Europe. Inglehart strongly emphasises the thesis that value systems of societies highly depend on economic development. Both dimensions are linked with economic development; self-expression values and secular-rational values are supported by economically developed societies, e.g., Germany, France, Britain, Italy, Japan, U.S., Sweden. Respectively, rather less economically developed countries such as India, Bangladesh, Morocco or Peru score high on survival and traditional values (economic development measured by GNP).

Besides the importance of economic development for value priorities, the cultural heritage plays a crucial role as well. The finding that Latin American countries rank high on traditional religious values and rank higher on self-expression values than their economic development would predict, could be traced back to the Iberian Colonial heritage that still persists centuries later.

European values map

Analogous to the World Values Map, a European Values Map has been plotted based on the survey results of the European Values Study. Again, the axes reflect the same two dimensions traditionalism vs. secular-rationalism and survival vs. self-expression. The meaning of the dimensions and the underlying items are identical with those of the just mentioned dimensions of the World Values Map.

[564] Inglehart and Welzel, "Changing Mass Priorities", 2010

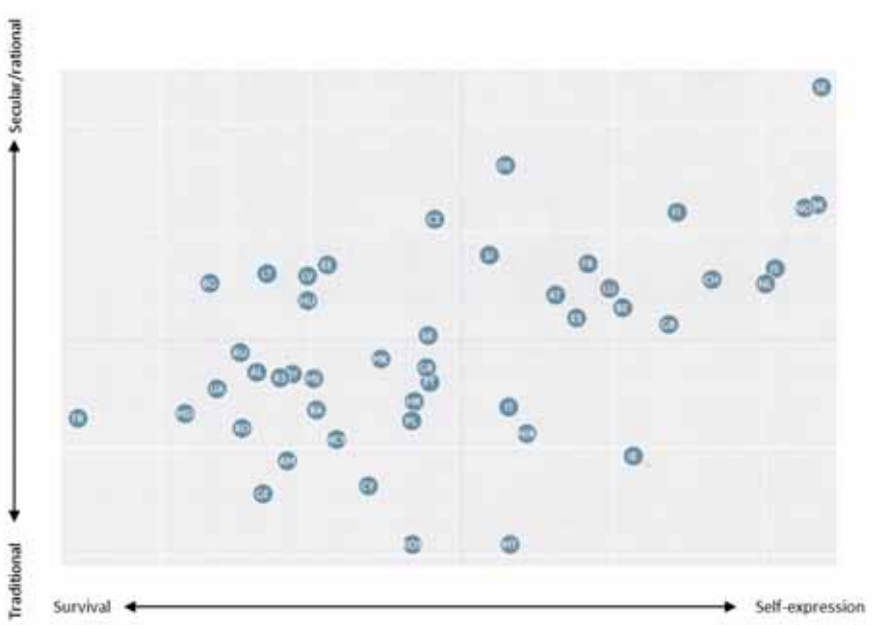


Figure 45: European values map based on the European values study[565]

The map reveals patterns of value priorities between the different European countries.[566] The geographically North Western (Netherlands, Belgium, Great Britain, Luxembourg) and Northern (Sweden, Denmark, Norway, Iceland, Finland) placed countries can be found in the top right quadrant. The Baltic States, together with some central European countries, can be found in the top left quadrant. Thus, both groups of countries rank high on secular-rational values. In addition, the North Western and Northern European countries rank high on self-expression values and the second group ranks high on survival values.

The bottom right quadrant, representing high scores on self-expression values and high scores on secular-rational values, is almost empty and in the bottom left quadrant the less prosperous countries are settled. As the theoretical approach of Inglehart suggests, the positioning of a country on the map can be explained by economic development and social-cultural heritages, languages, religious and ideological traditions. Protestant countries (Denmark, Sweden, Norway, Finland and Iceland) rank high on both dimensions, while the Roman Catholic countries (Italy, Portugal, Spain, France, Belgium and Austria) rather support traditional values. Furthermore the orthodox countries such as Romania, Armenia, Georgia and Moldova score lower on the survival/self-expression dimension than the Roman Catholic countries. In relation to the former East-West divide, it can be seen that all former communist countries can be found in the left hand side of the map, hence they score low on self-expression values and rather high on survival values. This may be due to the relatively recent collapse of the Soviet Union, which shattered their economic, social and political systems. Unsurprisingly, the mapping of countries in the European values map is quite similar to the positioning of European countries on the World values map.

7.4 ANALYSIS

In order to find patterns of differences or similarities between countries or groups of countries in Europe, a vast amount of value orientations could be used. Therefore it makes sense to

[565] Halman et al., Atlas of European Values, 2012.
[566] Ibid.

reduce the values that should be consulted for the context of PRISMS to those closely related to privacy and security. Privacy and security itself are concepts that have not been analysed in depth based on data from the EVS, WVS or ESS. Hence we will approach privacy and security by investigating related concepts that have been covered in greater detail, such as individualism, autonomy, authority and trust.

Though privacy and security are not directly covered, the existing value maps can be used as a starting point for analysis. As described above, the maps based on the European Values Study and the World Values Survey both reflect the traditional/secular-rational dimension and survival/self-expression dimension. In order to derive links between those value dimensions and privacy and security, it is worth studying the underlying items that reflect the respective value priority accompanying a specific scoring in the dimensions.

7.4.1 *Privacy*

The investigated Social Value Surveys do not cover "privacy" explicitly. For the purpose of approaching privacy indirectly, relations between *personal autonomy* and *individualism* and privacy are worth looking at. Both aspects play a role in the Social Value Surveys and offer possibilities of analysing differences in value orientations within Europe. The notion of privacy that might be drawn on is a rather broad notion such as "privacy of the person", since "privacy of the person is thought to be conducive to individual feelings of freedom and helps to support a healthy, well-adjusted democratic society".[567] Due to the indirect reference to privacy in the surveys it is not possible to break down notions of privacy any further.

Personal autonomy and individualism
It is commonly agreed that personal autonomy and privacy are two concepts that can be conceived as interrelated.[568] Privacy might be a result, as well as a prerequisite, of personal autonomy. Pauer-Studer perceives individual freedom and personal autonomy as constituting elements of liberal societies.[569] Privacy can be understood as "self-determination with respect to information about oneself" and the freedom to shape self-representation and identity formation.[570] Thinking in panoptic terms, privacy is an important aspect of guaranteeing autonomous behaviour that is not determined by the possibility of being watched.

Hagenaars et al. analysed data based on the European Values Study 1999/2000 and aggregated several covered items to the dimension of "personal autonomy". According to these authors countries or individuals with a high valuation of personal autonomy focus on the following aspects[571]: they are protest prone, children and marriage are not regarded as an absolute necessity and working women are highly accepted. Furthermore, they are tolerant to people from different ethnic backgrounds and also with regard to people with a deviant behaviour.

---

[567] Finn et al., 2013.
[568] This accounts at least for discussions relating to privacy and freedom. The emphasis is different if the focus lies on dignity. See: Whitman, James Q., "The Two Western Cultures of Privacy: Dignity Versus Liberty", *Yale Law Journal*, Vol. 113, 2003/04, pp. 1151-1221.
[569] Pauer-Studer, Herlinde, "Privatheit: Ein ambivalenter, aber unverzichtbarer Wert", in Peissl, Walter (ed.), *Privacy. Ein Grundrecht mit Ablaufdatum?*, Verlag der Österreichischen Akademie der Wissenschaften, Wien, 2003.
[570] Solove, 2008.
[571] Hagenaars, Jacques, Loek Halman and Guy Moors, "Exploring Europe's basic values map", in Arts, Wil, et al. (eds.), *The Cultural Diversity of European Unity*, Brill, Leiden, Boston, 2003.

The idea that individualism constitutes an inherent aspect of privacy is widely agreed upon. Hixson remarks that "the concept of privacy, as old as human history, tries to distinguish between the individual and the collective, between self and society. The concept is based upon respect for the individual, and has evolved into respect for individualism and individuality."[572] The fact that privacy is often viewed as an individual right supports the inherently individualistic aspect of privacy. Even the influential article "The Right to Privacy" written by Warren and Brandeis in 1890 already conceptualised privacy with a focus on the individual, which is reflected by the idea that privacy is "the right to be let alone"[573].

Whether individualistic tendencies have a civic or un-civic character is a contested question. Some see self-expression values as indicative of egoism and hence harmful for collective action[574], others see these values as implying a sense of human equality, and therefore an association with altruism.[575] In any case it can be assumed that individualism concerns privacy, and that societies where value priorities related to individualism are underpinned, privacy related issues play a crucial role as well.

The dimensions of the World Values Survey can serve as a reference point for the analysis of privacy related issues: Self-expression values are closely related to individualism. People who focus on self-expression values score high on the importance of individual freedom, the importance of subjective well-being and a high quality of life. Those values imply an individualistic nature, since the "pursuit of self-actualization and personal happiness is at the centre of value development and norm selection within an individualistic ethos".[576] Westin argues that privacy "is basically an instrument for achieving individual goals of self-realisation"[577].

The Human Values Scale which is part of the European Social Survey might also offer an entry point for approaching privacy. Hans Bay[578] used data derived from the first wave (2002) of the European Social Survey to develop a European value map. He focused on the responses to the 21-item Basic Human Values Scale and applied factor analyses, which resulted in two factors, which he named "Behaviourism in Society" and "Individual Possibilities".[579] The first factor (behaviourism in society) expresses the wish for the degree of acceptance with regard to society's norms and organisations. People loading high on this factor support the idea of proper behaving, the following of traditions and customs, the care for nature and environment, being humble and modest, to do what is told and to follow rules, and emphasise the equal treatment of people. The second factor (individual possibilities) expresses the respondent's wish in terms of personal possibilities of own success. People can be assigned to this factor if one supports statements that underpin the importance of being rich, to show abilities and be admired, to try new and different things in life, to have a good time, to make own decisions

[572] Hixson, Richard F., *Privacy in a public society: Human rights in conflict*, Oxford University Press, New York, 1987.
[573] Warren, Samuel D. and Louis D. Brandeis, "The Right To Privacy", *Harvard Law Review*, Vol. 4, No. 5, 1890, pp. 193-220.
[574] Flanagan, S. and A. R. Lee, "The new politics, culture wars, and the authoritarian-libertarian value change in advanced industrial democracies", *Comparative Political Studies*, Vol. 36, 2003, pp. 235-270.
[575] Inglehart and Welzel, 2005.
[576] Arts and Halman, 2004, p. 27.
[577] Westin, Alan F., *Privacy and freedom*, Atheneum, New York, 1967, p. 39.
[578] Bay, Hans, "European Value Map: Based on ESS Data", Paper presented at: Sixth International Conference on Social Science Methodology, Amsterdam, 16-20 August 2004.
[579] See ibid. for further information about methodology. In a 2007 paper presented at a conference in Florence he renamed the dimensions into "Social conformism" and "individualism".

and be free, to be successful, to seek adventures and to seek fun and things that give pleasures.

National differences
The World Values Map and the European Values Map show that countries which fall under the category "Protestant Europe", i.e., Sweden, Norway, Denmark, the Netherlands, Finland and Iceland, score high on self-expression values. Countries that score rather low on self-expression values and respectively high on survival values, are geographically located in the Eastern and Central part of Europe, namely Russia, Bulgaria, Ukraine, Romania, Latvia, Belarus and Serbia. Hence, it can be presumed that in the first group of countries, those that are geographically located in Northern Europe, the emphasis of self-expression values influences the perception of privacy. In turn, the same accounts for the latter group of countries. It can be assumed that the divergence of emphasis on self-expression values influences the perception of privacy issues.

According to Bay's investigation, the Scandinavian countries reflect a favour of "weak" government and "own traditions" and focus on individualism. Contrary to that, Greece and Spain are rather attached to traditions and religion. The Czech Republic is characterised by introverted individuals and little focus on money. Ireland is an example for a country where individuals are extroverted and the importance of money is stressed.

Hagenaars et al.'s analysis based on data of the European Values Study 1999/2000 develops the following countries as typical instances for socio-liberal and religious-normative countries: Ireland, Northern Ireland and Italy. Typical instances for the liberal, non-religious countries are Sweden and Denmark. Russia, Lithuania, Belarus, Estonia and Latvia form a cluster by being non-liberal and non-religious. Romania and Poland are assigned to be less liberal, more religious, normative countries. Some kind of grouping related to the geographic position of the countries are evident: Eastern/Central European countries are grouped together as well as the Western European countries. While the Eastern and Central European Countries (Russia, Lithuania, Hungary, Belarus, Estonia, Romania, Ukraine, Latvia, Poland, Slovakia, Bulgaria) are on the less socio-liberal, autonomous side of the continuum, the Western European (in terms of the former political blocs) countries (Spain, France, Finland, Italy, Austria, Northern Ireland, Ireland, Belgium, West Germany, Luxemburg, United Kingdom, Iceland, Denmark, the Netherlands, Sweden) can rather be found on the liberal, autonomous side. Exceptions from this tendency of country allocation are Portugal, Greece, and Malta, who are less autonomous and socio liberal than Croatia and Slovenia.

7.4.2 *Trust*

Another value orientation that is relevant for PRISMS is "trust". In contrast to "privacy" there is a direct reference to "trust" in the Social Value Surveys. Trust occurs in the European Social Survey, the European Values Study and the World Values Survey.

Definitions of trust
All three Values Surveys cover interpersonal trust; in addition the European Social Survey also covers institutional trust. Interpersonal trust, which can also be referred to as "general trust", is covered in almost the same way in the three value surveys: the wording of the question is "would you say that most people can be trusted, or that you can't be too careful in dealing with people?". Whilst the ESS uses a scale ranging from 0 to 10, the WVS and the EVS offer the two answers "most people can be trusted" and "you can't be too careful".

Besides this opposition between *trust in people* and *the need for carefulness in dealing with other people*, the surveys do not specify *trust* any further.

In general, as for instance Hudson defines it, interpersonal trust is related to choices "between trust and distrust and fully explicable as a product of rational behaviour"[580]. Contrary to that institutional trust can be understood as the extent to which people "trust the institution to fulfil its role in a satisfactory manner"[581]. An explicit definition of how institutional trust is supposed to be understood in the questionnaire is not given. Hence in the Social Value Surveys trust is understood in a rather general notion and there are not references to particular types of privacy or security.

The European Social Survey asks the following questions[582]:

> "Using this card, generally speaking, would you say that most people can be trusted, or that you can't be too careful in dealing with people? Please tell me on a score of 0 to 10, where 0 means you can't be too careful and 10 means that most people can be trusted.
>
> Using this card, please tell me on a score of 0-10 how much you personally trust each of the institutions I read out. 0 means you do not trust an institution at all, and 10 means you have complete trust.
>
> [national parliament,
> legal system,
> police,
> politicians,
> political parties,
> the European Parliament,
> the United Nations]"

The European Values Study[583] and the World Values Survey[584] ask the following question:

> "Generally speaking, would you say that most people can be trusted or that you can't be too careful in dealing with people?
> 1 Most people can be trusted
> 2 You can't be too careful (or Need to be very careful)"

The European Values Study furthermore differentiates between the following institutions:[585]

> "Please look at this card and tell me, for each item listed, how much confidence you have in them, is it a great deal, quite a lot, not very much or none at all?
>
> [the church,
> the armed forces,
> the education system,
> the press,
> trade unions,
> the police,

[580] Hudson, John, "Institutional Trust and Subjective Well-Being across the EU", *Kyklos*, Vol. 59, No. 1, 2006, pp. 43–62.
[581] Ibid.
[582] European Social Survey, "ESS Source Questionnaire Final (Round 5, 2010/11)", 2010.
[583] European Values Study, "EVS 2008 Master Questionnaire. Related to the Integrated Dataset Archive-Study-No. ZA4800, DOI:10.4232/1.10059", GESIS - Leibniz-Institut für Sozialwissenschaften, Mannheim, 2008.
[584] World Values Survey, "WVS 2010-2012 Questionnaire", 2011.
[585] European Values Study, 2008.

parliament,
civil service,
the social security system,
the European Union,
NATO,
United Nations Organization,
health care system,
the justice system,
major companies,
environmental organizations,
political parties,
government]"

National differences
Data from the European Values Study reveals that levels of interpersonal trust and levels of institutional trust differ across Europe.[586] In general, interpersonal trust throughout Europe is not very high. The highest level of trust can be found in Norway, Denmark, Sweden and the Netherlands, where on average between 60% and 70% of the population think that people can be trusted. Widespread distrust can be found in Northern Cyprus, Turkey, Albania and Kosovo, where fewer than 10% of individuals claim that most people can be trusted. Overall, the North Western countries show the highest level of interpersonal trust, followed by continental European countries, which in turn score higher than Mediterranean countries. Levels of interpersonal trust are lower in post-communist societies than in Western European Countries. A similar picture evolves when looking at the data based on the European Social Survey: Denmark, Sweden, Finland, Norway and The Netherlands show the highest amount of interpersonal trust, followed by Switzerland. The lowest amount of interpersonal trust can be found in Romania, Bulgaria, Slovakia and Serbia.

In relation to institutional trust, Iceland, Ireland, Malta, Denmark and Finland form a cluster with the highest levels of trust. In contrast, the Czech Republic, Greece, Bulgaria and Romania form a cluster with the lowest level of institutional trust. Western and Eastern European countries appear to resemble each other. Data based on the European Social Survey furthermore reveals a similar tendency, i.e., Eastern European countries rate low in terms of institutional trust, and the Northern European countries show a high level of institutional trust.

7.4.3 *Security*

In the three social value surveys analysed we found direct references to security as well as indirect references to security. The surveys cover security in a broad range of contexts, such as security in relation to employment, national security or secure surroundings.

Definitions of security
Security plays an important role within Inglehart's theory of value change, connecting economic security with personal value orientations. Materialist values prevail as long as basic human needs are not met. Those basic human needs can be connected to physical or socio-economic security and are reflected by the survival values measured in the World Values Survey. Respondents emphasising survival values rate high for instance on the following statements:[587]

[586] Arts and Halman, "European value changes in the second age of modernity", 2004.
[587] An overview of all items loading high on survival values is given in

"When seeking a job, a good income and safe job are more important than a feeling of accomplishment and working with people you like."

Government should take more responsibility to ensure that everyone is provided for.

The European Social Survey makes reference to security through the Human Value Scale, where security is operationalised as a basic human value with the core motivational goal of safety, harmony and stability of society, of relationships and of self. The items constituting security as a value in the Human Values Scale include:[588]

"Here we briefly describe some people. Please read each description and tick the box on each line that shows how much each person is or is not like you. How much like you is this person? [very much like me, like me, somewhat like me, a little like me, not like me, not like me at all]

It is important to him to live in secure surroundings. He avoids anything that might endanger his safety.

It is important to him that the government ensures his safety against all threats. He wants the state to be strong so it can defend its citizens."

Furthermore, the European Values Study investigates citizen's attitudes towards job security. The World Values Survey covers the things one has done for reasons of security (such as not to carry money, not to go out at night, to carry a knife, gun or other weapon), and the European Social Survey also broaches the issue of burglary, feelings of being safe and terrorism.

National differences

In order to detect differences in value orientations in relation to security between European countries, it is again worth looking at the World Values Map. Two dimensions for the World Values Map, the survival/self-expression dimension and the traditional/secular-rational dimension, reflect the prevailing value orientations in the respective country. In those countries that score high on survival values, economic and physical security is prioritized over self-expression and quality of life. This accounts for Baltic States and some Central European countries, i.e., Bulgaria, Latvia, Estonia, Lithuania and Hungary. According to Inglehart's approach the just mentioned countries also favour secular-rational values. Contrary to that, a couple of other countries emphasise survival values and traditional values, examples include: Romania, Moldavia, Armenia, Ukraine, Turkey and Georgia.

7.5 CONCLUSIONS AND SOME HYPOTHESES

Table 24.

[588] European Social Survey, "The European Social Survey, Self-completion questionnaire S-C-C (Round 4 2008)", 2008.

The primary aim of this task has been to analyse European and global Social Value Surveys and their results in terms of potential differences in prevailing value orientations related to privacy and security. We presume that conducting cross-national research without understanding how values shape people's perceptions and opinions on the subject would fail to capture essential information needed for a comprehensive analysis of survey results. Therefore this task supports the PRISMS survey in two manners: first, it points to differences in value orientations within Europe, which might directly affect perceptions of privacy and security. Such differences can for instance be traced back to historical experiences, cultural heritages, the political system or economic development and need to be taken into account when it comes to the interpretation of survey results. Second, this task contributes to the compilation of a list of demographic variables which are of interest for the PRISMS survey.

In this chapter, we have provided background information about values and values research by introducing common definitions and conceptual approaches to values. In addition we presented the most common approaches of how values can be measured, where in this task Social Value Surveys play a crucial role. The three surveys that have been investigated include the World Values Survey, the European Social Survey and the European Values Study, whose different methodological approaches and underlying theoretical ideas were presented.

In the analytical part of the task we followed an exploratory approach and investigated the surveys and studies based on those surveys with regard to privacy and security and related concepts. Our analysis revealed that privacy, security and trust are all covered with direct and indirect reference. Privacy is approached indirectly; trust directly and security directly and indirectly. Personal autonomy and individualism are concepts that have been covered by the surveys and are helpful to draw on in relation to privacy. Our analysis of social values surveys revealed that the surveys approach to operationalising privacy and security is somewhat different to those surveys analysed in Task 7.1 (chapter 3 and 5), where in social values surveys focus is placed on direct and indirect types of privacy and security.

As it became obvious, differences in value priorities in Europe exist. Based on our exploration, nationality, religiosity and socio-economic background might offer explanations for possible differences in value priorities. The work we did in this task leads us to the development of the following preliminary hypotheses:

1. *The higher the socio economic status of a citizen, the more important privacy is.*
2. *The economic development of a country determines citizen's perceived need for security mechanisms.*
3. *Security is always important, but the focus is different dependent on the higher the income.*

These hypotheses are developed based on the idea that economic security is connected with personal value orientations and that with growing economic security the importance of self-expression values increases too. As mentioned previously, self-expression values are connected to individualism and autonomy and therefore with privacy. As a consequence, privacy is valued higher by people who live in economically secure circumstances. Similarly, if the economic situation is difficult, survival values are emphasised and economic security is prioritised over self-expression values and quality of life.

4. *The religion of a citizen influences an individual's perception of privacy.*

As this task has revealed, the dominance of a religion in a country also influences value priorities and hence possibly perceptions of privacy and security. The emphasis on traditional values is strongly connected with religion. While Protestant countries rank high on self-expression and secular-rational values, Roman Catholic countries rather support traditional values. Also, orthodox countries score higher on survival values than Roman Catholic countries do.

5. *In those parts of Europe where interpersonal trust is low, citizens are willing to give up privacy for a potential increase in security.*

This hypothesis is based on the knowledge that interpersonal trust is low in those countries where survival values play an important role. Hence the argumentation follows the explanations above.

Finally we conclude that the social value surveys we analysed do offer interesting insights into differences in terms of value priorities related to privacy and security. Yet it should be kept in mind that the concepts relevant for PRISMS are not the focus of the surveys we investigated. Approaches to privacy and security are either rather broad or very specific, which justifies our exploratory development of hypotheses.[589]

[589] Additional hypotheses and a cluster of European countries can be found in Annex 2 and 3.

Chapter 8: Recommended questions

Hayley Watson, David Wright and Rachel Finn
Trilateral Research & Consulting, LLP

8 RECOMMENDED QUESTIONS

The aim of this chapter (Task 7.3) was to review and analyse survey question techniques to support the construction of the PRISMS survey. The partners have done so by reviewing questions used in other surveys discussed in Task 7.1., chapter 4 of this report. We have proposed a set of hypotheses and related questions that could be used in the PRISMS survey.

As mentioned by Bryman, the wording of a question is a crucial consideration in the use of a survey as a method of social research.[590] However, as noted by Judd et al., creating useful questions is one of the most complex tasks in the construction of a survey.[591] For Judd et al., researchers should have a "clear conceptual idea of what is to be measured". Without this clear understanding of what is to be measured, researchers are unlikely to obtain valid and reliable data that will be useful in addressing their research goals.[592] For researchers to have a conceptual understanding of what should be measured, they must go through the process of operationalising their concepts. Operationalisation involves defining the key concepts under investigation.[593] For instance, in relation to PRISMS, key concepts for partners include: privacy, trust, security and surveillance. Accordingly, partners should try to define these terms and develop ways of understanding public opinion in relation to these areas of concern. A secondary aim of this report was to explicate how past surveys have formulated questions about privacy, trust, security and surveillance. Such an explication may help in devising questions to be used in the PRISMS survey.

For PRISMS, not only do partners need to understand the way in which privacy, trust, security and surveillance have been defined, but also partners need to understand the ways in which public attitudes are measured in relation to these concepts. Thus, the indicators used in surveys are of interest. As Bryman suggests, indicators offer researchers a way of measuring concepts.[594] For Bryman, an indicator is "a measure that is employed to refer to a concept when no direct measure is available".[595] For instance, as will be observed in section 8.1, researchers have had to develop indicators to measure the concept of "privacy" of data and images. A common survey technique for measuring attitudes is through the use of what Judd et al. refer to as an "attitude scale", often in the form of a Likert scale.[596] Likert scales are commonly used in social science research, and offer researchers the opportunity to ask respondents the degree to which they believe something.

Accordingly, this section will proceed in two sub-sections. First, the partners will return to the findings of Task 7.1 to examine how surveys have operationalised the four key concepts relevant to the PRISMS survey: privacy, trust, security and surveillance. Partners will also investigate the various ways in which attitudes have been measured in relation to privacy, trust, security and surveillance. Second, in 8.2, partners will formulate hypotheses and related questions surrounding the complex relationship between privacy, trust, security and surveillance to assist those responsible for designing the PRISMS survey in ensuring that appropriate questions are asked. Furthermore, partners will recommend and outline questions analysed or identified during PRISMS Task 7.1 that could be used in the PRISMS survey.

[590] Bryman, Alan, *Social Research Methods*, 3rd ed., Oxford University Press, Oxford, 2008.
[591] Judd, Charles, M., Eliot Smith R., and Louise Kidder H., *Research Methods in Social Relations*, 6th ed., Holt, Rinehart & Winston, London, 1991.
[592] Ibid., p. 235.
[593] Bryman, 2008.
[594] Ibid., p. 145.
[595] Ibid., p. 694.
[596] Judd et al., 1991, p. 232.

8.1 OPERATIONALISATION OF CONCEPTS

In this sub-section, the partners review how other surveys have defined and developed questions to measure public attitudes towards privacy, trust, security and surveillance.

8.1.1 *Privacy*

Finn, Wright and Friedewald have presented a typology of seven different types of privacy, as follows:[597]

- *Privacy of the person* encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private.
- *Privacy of behaviour and action* concerns activities that happen in public space and private space.
- *Privacy of communication* aims to avoid the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to e-mail messages.
- *Privacy of data and image* includes protecting an individual's data from being automatically available or accessible to other individuals and organisations and ensuring that people can "exercise a substantial degree of control over that data and its use".
- *Privacy of thoughts and feelings* includes individuals having the right to think whatever they like.
- *Privacy of location and space* argues that individuals have the right to move about in public or semi-public space without being identified, tracked or monitored.
- *Privacy of association (including group privacy)* concerned with people's right to associate with whomever they wish, without being monitored.

As the following table indicates (Table 25), of the surveys analysed in Task 7.1, surveys are most likely to consider five of these types of privacy: privacy of the person, privacy of behaviour and action, privacy of communication, privacy of data and image and privacy of location and space:

Table 25: Types of privacy and existing surveys

Type of privacy	Existing surveys
Privacy of the person	• *State of the Nation* • *Globalization of personal data project* • *Unisys Security Index* • *Financial Times/Harris Poll: Body scanners*
Privacy of behaviour and action	• *Special 9/11 Poll* • *URBANEYE: CCTV in Europe* • *Personlig Integritet: Perceptions of privacy in public spaces* • *The Globalization of personal data project* • *Special Eurobarometer 359: Data protection and e-Identity*

[597] Finn, Rachel, David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert et al. (eds.), *European data protection: coming of age?*, Springer, Dordrecht, 2013.

Type of privacy	Existing surveys
Privacy of communication	• *Special 9/11 Poll* • *Flash Eurobarometer 225: Citizens perceptions of data protection* • *The Globalization of personal data project* • *Canadians and Privacy* • *State of the Nation* • *Special Eurobarometer 359: Data protection and e-Identity*
Privacy of data and image	• *Eurobarometer 46.1: Information technology and privacy* • *Special 9/11 Poll* • *Survey on citizens trust in ID Systems and Authorities* • *PEW Internet & American Life: Digital Footprints* • *Flash Eurobarometer 225: Citizens perceptions of data protection* • *Personlig Integritet: Perceptions of privacy in public spaces* • *The Globalization of personal data project* • *Canadians and Privacy* • *Privacy 2.0* • *State of the Nation* • *PEW Internet & American Life: Reputation Management* • *EU Kids Online: Risks and Safety on the Internet* • *Special Eurobarometer 359: Data protection and e-Identity* • *Online Profile & Reputation Perceptions Study* • *Internet Privacy Research*
Privacy of location and space	• *Special 9/11 Poll* • *URBANEYE: CCTV in Europe* • *The Globalization of personal data project*

As indicated above, 15 of the 17 surveys focus on privacy of data and image. Surveys that focused on other types of privacy often relied upon surveillance technology examples in lieu of a definition of privacy. Thus, by reviewing surveys relating to privacy, we have been able to identify a gap in current public opinion polls and the way in which they operationalise the term "privacy".

In our review of the 17 surveys that assessed public attitudes towards issue of privacy, we found that11 defined "privacy". *Eurobarometer 46.1: Information technology and privacy* explored privacy by trying to understand the "personal tracks" of individuals' activities and what this meant for the privacy of their personal data. Over time, we can see the move towards the use of the term "personal information", and eight of the 11 surveys defined privacy in relation to an individual's "personal information". For instance, *Flash Eurobarometer 225: Citizens perceptions of data protection* used the following question to gather individuals' perceptions of the security of their "privacy": [598]

> Different private and public organisations keep personal information about people. Are you concerned or not that your personal information is being protected by these organisations?
>
> • Very concerned
> • Fairly concerned

[598] The Gallup Organization, 2008, p. 7.

- Not very concerned
- Not at all concerned
- DK/NA

In the question above, researchers used a scale to measure respondents' "concern" over the security of their personal information. Researchers accounted for a full range of responses, particularly in relation to providing respondents with a neutral option from which to choose where if they were unable to answer the question. Such a technique enables researchers to gather valid results, as respondents would not be restricted to providing an answer that they may not have felt was applicable to their views.[599]

Some surveys chose to provide respondents with examples of cases in which their privacy might be affected. For instance, the *PEW Internet & American Life Project: Digital Footprints* survey provided the following examples to ask people how important privacy was to them:[600]

- Controlling who has access to your personal information
- Not being monitored at work
- Having individuals in social and work setting not ask you things that are highly personal.

As Bryman says, to ensure greater validity of results, researchers should avoid the use of technical terms that respondents may not understand.[601] Accordingly, rather than take it for granted that individuals understand what is meant by privacy, the use of examples, may, for some, clarify what is meant by the term being used, thereby helping respondents to provide more accurate and valid responses to the questions they are being asked. However, the use of examples need to be carefully chosen and translated in such a way as to uphold the validity of the question.

Some surveys also discussed "privacy of the person" in relation to the individual's attitude towards the introduction of surveillance technologies, such as full body scanners to enhance security, bank issued smart cards to prevent identity theft or the collection of DNA samples to identify criminals. The 2010 *Financial Times/Harris Poll: Body scanners* asked respondents how they felt about the use of full body scanners in airports:[602]

> Following the failed attempt to explode a bomb on a plane in America on Christmas day, certain measures to increase not only airline security, but also security measures in other locations, are being discussed. How much do you agree or disagree with the following statements about some of these measures?' 1. Body scanners that X-ray the full body should be introduced at airports.
>
> - Strongly agree
> - Somewhat agree
> - Somewhat disagree
> - Strongly disagree
> - Neither agree nor disagree

A second question from this poll is:[603]

[599] Judd et al., 1991.
[600] Madden, et al., 2007, p. 2.
[601] Bryman, 2008.
[602] Harris Interactive, 2010, p. 3.
[603] Ibid.

> Following the failed attempt to explode a bomb on a plane in America on Christmas day, certain measures to increase not only airline security, but also security measures in other locations, are being discussed. How much do you agree or disagree with the following statements about some of these measures?' 3. There is already too much surveillance of individuals by the government.
>
> 1. Strongly agree
> 2. Somewhat agree
> 3. Somewhat disagree
> 4. Strongly disagree
> 5. Neither agree nor disagree

The two questions used within the survey move from general questions, which could be perceived as somewhat leading question with their use of examples, about understanding public attitudes towards the installation of scanners, to more specific questions aimed at addressing public attitudes to surveillance in general. However, the questions included in the survey do not explicitly mention privacy. Accordingly, the researchers missed an opportunity to fully establish a clear understanding of the link between privacy of the person and the installation of surveillance technologies, in the form of scanners, to enhance security. Within the PRISMS survey it will be necessary to carefully balance the two issues (privacy and security) whilst avoiding unnecessarily leading participant responses. In terms of the measurement of public attitudes, researchers who created this question employed a Likert scale and provided respondents with an opportunity to provide a neutral opinion.

Elsewhere, *State of the Nation* (2010) also asked respondents about privacy of the person in relation to biometric measures of DNA. Respondents were asked how long authorities should keep individuals' DNA following their conviction. The question helped researchers to understand differences in opinion according to different types of convictions. However, the researchers did not explicitly define privacy:[604]

> In England and Wales, the police can currently take a DNA sample from anyone arrested for a recordable offence before they are charged with an offence. This sample is analysed to produce a DNA profile which is kept permanently on a database, whether or not the person is convicted or even charged with an offence. For each of the following please tell me whether you think the police should keep a person's DNA profile on the database permanently, or whether there should be a time limit.
>
> - If they are convicted of a serious violent or sexual offence, such as rape or murder
> - If they are convicted of burglary
> - If they are convicted of being drunk and disorderly, or taking part in an illegal demonstration

However, this question is not quite precise since the respondent did not have the option to express his opinion whether there should be a time limit. Researchers only gave respondents an option to choose the type of offence for which an individual's DNA could be kept in the database for however long.

[604] The Joseph Rowntree Reform Trust Ltd. and ICM, 2010, p. 6.

Some surveys made an effort to understand "privacy of communication" by asking individuals about their privacy concerns in relation to surveillance. For instance, the *Canadians and Privacy* (2009) survey asked respondents:[605]

> How concerned are you about the impact of new technologies on your privacy? Please use a 7 point scale where 1 means not at all concerned, 7 means extremely concerned and the mid-point 4 means somewhat concerned.
>
> 1. Not at all concerned
> 2. .
> 3. .
> 4. Somewhat concerned
> 5. .
> 6. .
> 7. Extremely concerned
>
> DK/NR

Within this survey, "new technologies" relating to communication included: online social networking sites, cell phones and telecommunications.[606] Again, unlike many surveys focused on data privacy, this question does not provide participants with any indication of what is meant by the term "privacy". As in the question (above) researchers involved in designing this survey used a Likert scale to understand public attitudes towards concern, and once again, included a "don't know" (DK) and no response (NR) option.

Elsewhere, in the *Flash Eurobarometer 225: Citizens perceptions of data protection,* in contrast to the *Canadians and Privacy* (2009) survey, researchers asked an indirect question about privacy of communication by asking respondents whether or not, in the fight against international terrorism, they felt that it was appropriate to monitor people's telephone calls. In addition, the survey asked respondents questions relating to privacy of personal data in the form of Internet use, credit card use and monitoring of people's details when they fly:[607]

> In light of the fight against international terrorism, do you think that, in certain circumstances, should it be possible:
>
> - to have people telephone calls monitored?
> - to have people's internet use monitored?
> - to have people's credit card use monitored?
> - to have people's details monitored when they fly?

As seen in the question above, the question does not directly ask people about their perceptions towards privacy, rather, it is a silent backdrop to what they are being questioned; however, in this question, the intention to ask about privacy of communication is more explicit. During the survey, researchers trying to understand attitudes towards ensuring security predominantly focus their attention on questions relating to privacy of data and image, rather than other types of privacy.

"Privacy of location and space" and "privacy of behaviour and action" were also commonly discussed in relation to individuals' attitudes towards the impact of surveillance technologies on their privacy. For instance, the 2002 *Special 9/11 Poll* directly asked respondents about privacy in the context of visual surveillance measures such as CCTV and the impact such

[605] EKOS Research Associated Inc., 2009, p.6 (Appendix A).
[606] Ibid., p. 6 (Appendix A).
[607] The Gallup Organization, 2008, p. 135.

measures might have on their civil liberties, however, the term "civil liberties" was not defined:[608]

> Following are some increased powers of investigation that law enforcement agencies might use when dealing with people of terrorist activity, but which would also affect our civil liberties. For each please indicate whether you would favour or oppose it.

	Favour	Oppose	Don't Know
Adoption of a national I.D. system for all U.S. citizens			
Expanded camera surveillance on streets and in public spaces			
Law enforcement monitoring of Internet discussions in chat rooms and other forums			
Expanded government monitoring of cell phones and email to intercept communications			

As seen in the question used in the *Special 9/11 Poll* (above) once again, researchers supply respondents with the opportunity to provide a neutral response, thereby enhancing the validity of responses by not forcing respondents to provide an answer that they may not want to provide.

Elsewhere, the *Special Eurobarometer 359: Data protection and e-Identity* survey asked respondents about "privacy of behaviour and action" using questions that seek to understand attitudes towards the recording of behaviour. Researchers formulated questions that avoid asking respondents about one particular type of privacy, in this case, privacy of behaviour and action. In addition, to the survey asked respondents about their attitudes towards privacy of location and space, privacy of communication and privacy of data:[609]

> QB13. Nowadays, cameras, cards and websites record your behaviour, for a range of reasons. Are you very concerned, fairly concerned, not very concerned or not at all concerned about your behaviour being recorded…?
>
> - Via payment cards (location and spending)
> - Via mobile phone/mobile Internet (call content, geo-location)
> - In a private space (restaurant, bar, club, office etc.)
> - Via store or loyalty cards (preferences and consumption, patterns etc.)
> - On the Internet (browsing, downloading files, accessing content online)
> - In a public space (street, subway, airport etc.)

Our review of existing surveys revealed that some individuals are concerned about the impact of the growing number of surveillance technologies on their lives, particularly in relation to the type of surveillance measure under discussion. However, surveillance measures were not always discussed in relation to privacy. The following table shows whether existing surveys analysed in Task 7.1 included any questions that asked respondents how they felt about supporting enhanced surveillance measures in relation to both security and privacy, thereby operationalising the two concepts into a single question.

[608] Taylor, 2002, p.3.
[609] TNS Opinion and Social, 2011, p. 64.

Table 26: Surveillance, security and privacy

Survey	Support increasing surveillance measures to enhance security	Concerned about impact of surveillance technologies on privacy
Special 9/11 Poll	Yes	Not Questioned
A two-edged sword: video surveillance in Helsinki	Yes	Not Questioned
URBANEYE – CCTV in Europe	Yes*	Some (41.4%)
e-Identity: attitudes towards biometrics	Yes	Not Questioned
Flash Eurobarometer 225: Citizens perceptions of data protection	Yes	Not questioned
Personlig Integritet: Perceptions of privacy in public spaces	Yes	Some*
The Globalisation of Personal Data	Yes	Some (37.8%)
Canadians and Privacy	Unclear	Yes
State of the Nation	Some	Not Questioned
Financial Times/Harris Poll: Body Scanners	Yes	Not Questioned
Special Eurobarometer 359: Data protection and e-Identity	Not Questioned	Not Questioned

*Different results in different countries.

As shown in Table 26 above, some surveys asked respondents how they felt about increasing surveillance measures to enhance security. However, they did not include a question asking respondents whether this impacts their sense of privacy. Thus, many existing surveys do not fully explore the relationship between surveillance and privacy. One survey that did explore surveillance technologies and its impact on privacy in a single question was the 2009 *Canadians and Privacy* survey:[610]

> Are there any new technologies that you are particularly concerned about with respect to privacy issues? If so, which ones?
>
> - Internet/computer use
> - Hacking technologies/invasion of privacy/identity theft
> - Credit cards/debit card concerns of transactions
> - Surveillance/tracking/recording technologies
> - Banking/online banking
> - Use of cell phone/telecommunications technology
> - Online social networking sites
> - Companies/orgs selling information
> - DK/NR

In addition to asking about surveillance technologies in relation to privacy, as revealed by the *Canadians and Privacy* survey, future research could try to determine the extent of an individual's understanding of the nature of surveillance technologies and what this means for an individual's privacy. During the analysis of existing surveys in PRISMS Task 7.1, we found that some surveys show that individuals do care where CCTV cameras are located, and how this location may impact their privacy. For instance, citizens appear to be more supportive of the use of cameras in public spaces, not private spaces (see, for instance, *URBANEYE: CCTV in Europe* and *A two-edged sword: video surveillance in Helsinki*, *Flash*

[610] EKOS Research Associated Inc, 2009, p. 16.

Eurobarometer 225: Citizens perceptions of data protection). This finding provides evidence of the importance of understanding public attitudes towards surveillance technologies in relation to privacy, not just security, which is something to be taken into account in the PRISMS survey.

The surveys analysed for PRISMS Task 7.1 did not always consult individuals on all seven types of privacy. In particular, none of them considered privacy of thoughts and feelings or privacy of association (including group privacy). This over-reliance on privacy of data and image needs to be countered by a consideration of other, additional important aspects of privacy. In addition, when asking respondents about issues such as surveillance technologies that impede an individual's privacy, some surveys failed to include a question to assess how individuals felt about these surveillance measures in relation to their sense of privacy. Accordingly, there is no opportunity to understand the relationship between the two. In terms of measuring public attitudes towards privacy, researchers commonly used Likert scales and included an option for respondents to provide a neutral response to their questions, thereby enhancing the validity of responses. We suggest that the PRISMS survey take into account the seven types of privacy; further details can be found in section 8.2.

8.1.2 *Trust*

Our analysis of surveys found that those who designed the surveys often did not define the concept of "trust". Rather, trust appears to be a common sense term, in that respondents will understand what is meant by the term when it is asked. A useful definition of trust can be found in a report on surveillance by the UK's House of Commons Home Affairs Committee, who defines trust "predominantly to mean confidence in and reliance on the capabilities and good faith of a person or organisation".[611] Within the construction of the PRISMS survey it will be necessary to clarify which element of trust focus will be placed on.

During the review of surveys, the authors found that trust is commonly defined in relation to one particular type of privacy: the privacy of data and images, where individuals are asked whether they trust others to secure their personal data. Thus, the surveys mention trust in relation to both privacy and security. For instance, the *Flash Eurobarometer 225: Citizens perceptions of data protection*, asked:[612]

> I am going to read you a list of (NATIONALITY) organisations that may keep personal information about you. Please tell me if you trust or do not trust each of them to use your personal information in the proper way.
>
> 1. Trust
> 2. Does not trust
> 3. DK/NA

As seen in the question above, as with questions relating to privacy, researchers used a neutral response to give those respondents that were unsure of an alternative option to select. A second example is contained in the following question posed by the *Globalization of personal data project*, where the term "protection" points towards the concept of security and researchers used a neutral response within a Likert scale to measure responses:[613]

---

[611] House of Commons Home Affairs Select Committee, *A Surveillance Society?*, Fifth Report of Session 2009-10, HC 58-I, The Stationery Office, London, 8 June 2008, p. 38.
[612] The Gallup Organization, 2008, p. 10.
[613] Zureik et al., 2010, p. 365.

What level of trust do you have that private companies, such as banks, credit card companies and places where you shop, will protect your personal information?

1. Very high level of trust
2. Reasonably high level of trust
3. Fairly low level of trust
4. Very low level of trust
5. Not sure

As seen in the question above, this question surrounding "trust" is operationalised in a different way to the *Flash Eurobarometer 225: Citizens perceptions of data protection*. Researchers from the *Globalization of personal data project* provide respondents with further information relating to where and when personal information about them might be gained. In addition, respondents are provided with a greater range of options from which to choose in relation to the extent of their trust towards private companies, and are therefore not limited to simply saying they do or do not trust them.

Alternatively, the following question asked by researchers in the *Special Eurobarometer 359: Data protection and e-Identity* employs a combination of the previous two styles of questioning. The question (below) provides respondents with a question relating to trust as well as a range of responses for respondents from which to choose in relation to different types of authorities and private companies: [614]

QB 25. Different authorities (government departments, local authorities, agencies) and private companies collect and store personal information. To what extent do you trust the following institutions to protect your personal information?

- Health and medical institutions
- National public authorities (e.g., tax authorities, social security authorities)
- Banks and financial institutions
- European institutions (European Commission, European Parliament, etc.)
- Shops and department stores
- Phone companies, mobile phone companies and Internet Services Providers
- Internet companies (Search engines, Social Networking Sites, E-mail Services)

The respondents were provided with five options from which to choose: "totally trust", "tend to trust", "tend not to trust", "do not trust at all" and "DK".[615] In all three instances, trust is operationalised in relation to the protection and handling of personal data; little attention is paid to trust in relation to other matters of privacy.

This is again seen in survey questions included by researchers in the *Eurobarometer 46.1: Information technology and privacy,* where *trust* was discussed in an indirect fashion. Questions in this survey asked whether citizens would want a say in the handling of their data, which implies a line of questioning of whether they trust others with their data:[616]

Which one or two of the following opinions come closest to your own?

A. It has to be possible to get access to the services on these networks by giving no or very little personal information

[614] TNS Opinion and Social, 2011, p. 17 (Appendix - Questionnaire).
[615] Ibid., p. 17 (Appendix - Questionnaire).
[616] INRA (Europe), 1997, p. 24.

B. I always want to know who has information about me and what they intend to do with it
C. I want to be able to give my agreement before information about me is used
D. It does not matter to me what is done with my personal information, if it enables me to use a new service
E. If I am told in advance, it does not bother me if companies use information about me to send me advertising leaflets
F. I want the tracks that I leave on the networks when I use these new technologies to remain confidential or to be erased automatically so that no one can use them
G. None of these.

During PRISMS Task 7.1, partners found that the surveys did not pay attention to the relationship between trust, privacy and surveillance technologies. Rather, partners found that trust is predominantly discussed in relation to the one particular type of privacy, privacy of data and images. Additionally, partners found that the concept "trust" was not operationalised; rather it was regarded as a common sense term, where researchers took it for granted that participants would understand what was meant by the term. Of the surveys analysed, partners found that attitudes in relation to trust were commonly measured using a Likert scale with the inclusion of a neutral option. In section 8.2, partners will provide a definition of "trust" when providing an example of a question to be used.

8.1.3 *Security*

The first PRISMS work package developed a taxonomy of "security" that categorised security into seven different types.[617] These included: physical security, political security, socio-economic security, cultural security, environmental security, radical uncertainty and information security. As the following table shows (Table 27), the surveys assessed in PRISMS Task 7.1 were commonly focused on three types of security: physical, radical uncertainty and cyber and information. In addition, one survey assessed economic security. These types of security have been defined as:

- *Physical security:* That part of security concerned with physical measures designed to safeguard the physical characteristics and properties of systems, spaces, objects and human beings.

- *Radical uncertainty security:* That part of security concerned with measures designed to provide safety from exceptional and rare violence/threats, which are not deliberately inflicted by an external or internal agent, but can still threaten drastically to degrade the quality of life.

- *Cyber and information security:* That part of security concerned with measures designed to protect information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

- *Socio-economic security:* That part of security concerned with economic measures designed to safeguard the economic system, its development and its impact on individuals.[618]

[617] Friedewald, 2012.
[618] Lagazio, 2012, pp. 17-19.

Table 27: Types of security and existing surveys

Type of security	Existing surveys
Physical security	• *Special 9/11 Poll* • *A two-edged sword: video surveillance in Helsinki* • *URBANEYE – CCTV in Europe* • *Flash Eurobarometer 225: Citizens perceptions of data protection* • *The Globalization of personal data project* • *Canadians and Privacy* • *State of the Nation* • *Financial Times/Harris Poll: Body Scanners* • *Unisys Security Index* • *EU Kids Online*
Economic security	• *Unisys Security Index*
Radical uncertainty security	• *Special 9/11 Poll* • *Flash Eurobarometer 225: Citizens perceptions of data protection* • *Financial Times/Harris Poll: Body Scanners*
Cyber and information security	• *E-Identity: attitudes towards biometrics* • *Flash Eurobarometer 225: Citizens perceptions of data protection* • *Unisys Security Index* • *EU Kids Online* • *Special Eurobarometer 359: Data protection and e-Identity* • *Online Profile & Reputation Perceptions Study*

Thus, within the analysis of surveys in PRSIMS Task 7.1, the concept of security was commonly defined in one of three ways (with the exception of the *Unisys Security Index* which refers to financial security) and often in relation to surveillance. Surveys that include reference to physical security, such as *A two-edged sword: video surveillance in Helsinki* and *The Globalization of personal data project* commonly attribute security to crime. For instance, the following Likert scale was used within *The Globalization of personal data project* survey: [619]

> Some communities and private companies are using surveillance cameras, also known as closed circuit televisions or CCTVs to monitor public places in order to deter crime and assist in the prosecution of offenders. In your opinion, how effective are the following CCTVs in reducing crime?

Randomize list	Very effective	Somewhat effective	Not very effective	Not effective at all	Not sure
Community CCTVs (such as outdoor camera in public places)					
In-store CCTVs					

Alternatively, the *State of the Nation* asked people about their view of surveillance technologies, in the form of DNA and whether certain types of criminals (e.g., those convicted of rape, burglary, murder, drunk and disorderly conduct or taking part in an illegal

[619] Zureik et al., 2010, p. 371.

demonstration) should have their DNA records kept on file permanently.[620] Here surveillance is used to combat rather than deter crime. Thus, in some surveys such as the *State of the Nation* and the *Globalisation of Personal Data,* rather than being asked about experiences of threats to physical security, individuals are presented with questions referring to aspects of physical security and surveillance. In this way, it appears as though researchers are using security to help operationalise surveillance.

In addition to physical security, surveys that alluded to radical uncertainty security, such as *Special 9/11 Poll, Flash Eurobarometer 225: Citizens perceptions of data protection* and the *Financial Times/Harris Poll: Body Scanners*, also used the threat of radical security to ask respondents about their perceptions of surveillance technologies. Thus, attention remains on perceptions of surveillance rather than researchers' trying to understand attitudes towards actual security.

Other surveys, such as the *EU Kids Online* survey, directly ask respondents about their experiences with online security in the context of bullying or child exposure to sexual content. The following question was used:[621]

> Sometimes children or teenagers say or do hurtful or nasty things to someone and this can often be quite a few times on different days over a period of time, for example. This can include: teasing someone in a way this person does not like; hitting, kicking or pushing someone around; leaving someone out of things. Has someone acted in this kind of hurtful or nasty way to you in the past 12 months? QC113: How often has someone acted in this kind [hurtful and nasty] way towards you in the past 12 months?
>
> - More than once a week
> - Once or twice a month
> - Less often
> - Not at all

In addition, the *EU Kids Online* survey also asked respondents about their exposure to cyber and information security:[622]

> Do you think there are things on the internet that people about your age will be bothered by in any way? In the past 12 months, have you seen or experienced something on the internet that has bothered you in some way?

As seen in *Flash Eurobarometer 225: Citizens perceptions of data protection* and the *Unisys Security Index*, researchers often refer to threats to individuals in the form of data breaches online and identity theft (although identity theft can be seen as a threat to physical security as well). The following question was used in the *Flash Eurobarometer 225: Citizens perceptions of data protection*:[623]

> Do you think that transmitting your data over the Internet is sufficiently secure?
>
> 1. Yes
> 2. No
> 3. Does not use the Internet/has no computer
> 4. DK/NA

[620] The Joseph Rowntree Reform Trust Ltd. and ICM, 2010, p. 6.
[621] Livingstone et al., 2010, p.67.
[622] Ibid., p. 103.
[623] The Gallup Organization, 2008, p. 134.

Thus, as with the operationalisation of the concept of privacy, partners have found that the operationalisation of security is limited within existing surveys. Public attitudes towards security are commonly investigated using Likert scales. As with the measuring of attitudes towards privacy and trust, partners have found that when measuring public attitudes towards security survey designers have included a response options that enables respondents to provide a neutral response to the questions they are asked. In relation to the PRISMS survey, partners would advise the survey designers to adhere to taxonomy of security previously identified in Work Package 1. Further information regarding recommendations relating to the PRISMS survey and security can be found in section 8.2.

8.1.4 *Surveillance*

Central to our work on PRISMS is how other surveys have defined the concept "surveillance". As identified by the partners in PRISMS Task 7.1, the majority of surveys (nine out of 12) directly refer to surveillance by developing a wider understanding of what is meant by the term by providing audiences with examples of surveillance technologies, such as cameras and biometrics. The following example is from the 2010 *Financial Times/Harris Poll: Body Scanner*: [624]

> Following the failed attempt to explode a bomb on a plane in America on Christmas day, certain measures to increase not only airline security, but also security measures in other locations, are being discussed. How much do you agree or disagree with the following statements about some of these measures?' 1. Body scanners that X-ray the full body should be introduced at airports.
>
> - Strongly agree
> - Somewhat agree
> - Somewhat disagree
> - Strongly disagree
> - Neither agree nor disagree

Some surveys have defined the concept of surveillance in relation to investigative techniques that may impact civil liberties, and thereby link surveillance with issues surrounding privacy, as seen in the *Special 9/11 Poll*:[625]

> Following are some increased powers of investigation that law enforcement agencies might use when dealing with people of terrorist activity, but which would also affect our civil liberties. For each please indicate whether you would favour or oppose it.

	Favour	**Oppose**	**Don't Know**
Adoption of a national I.D. system for all U.S. citizens			
Expanded camera surveillance on streets and in public spaces			
Law enforcement monitoring of Internet discussions in chat rooms and other forums			
Expanded government monitoring of cell phones and email to intercept communications			

[624] Harris Interactive, 2010, p. 2.
[625] Taylor, 2002, p. 3.

As seen in the question above, question designers have provided respondents with three options to choose from, including a neutral option.

The Eurobarometer studies use a different technique, for example, by referring to monitoring (as seen in the *Flash Eurobarometer 225: Citizens perceptions of data protection)* or recording of behaviour (as seen in the *Special Eurobarometer 359: Data protection and e-Identity)*. The term surveillance is not directly employed in either Eurobarometer; the following example, from the *Special Eurobarometer 359: Data protection and e-Identity* provides further evidence of researchers not using the term "surveillance":[626]

> Nowadays, cameras, cards and websites record your behaviour, for a range of reasons. Are you very concerned, fairly concerned, not very concerned or not at all concerned about your behaviour…?
>
> - Very concerned
> - Fairly concerned
> - Not very concerned
> - Not at all concerned
> - Not applicable
> - Don't know

As seen in the question from the (above) researchers have employed a Likert scale around the measure of "concern" to understand public attitudes towards this issue. Alternatively, rather than focusing on recording of behaviour, the (earlier) *Flash Eurobarometer 225: Citizens perceptions of data protection* focuses its attention on privacy of data, and thus asks about surveillance in relation to monitoring. Here a Likert scale is once again used by researchers, but this time in relation to who should be monitored:[627]

> In light of the fight against international terrorism, do you think that, in certain circumstances, it should be possible:
> a) to have people's telephone calls monitored?
> b) to have people's internet use monitored?
> c) to have people's credit card use monitored?
> d) to have people's details monitored when they fly?
>
> - No
> - Yes, but only people who are suspected of terrorist activities
> - Yes, but even suspected terrorists should only be monitored under the supervision of a judge or with equivalent safeguards
> - Yes, in all cases
> - DK/NA

As identified in PRISMS Task 7.1, it is possible to understand surveillance in relation to the various types of surveillance technologies that exist. In the FP7 SAPIENT project, researchers defined a typology of surveillance technologies that might be useful to the design of the PRISMS survey. Different types of surveillance technologies include: visual surveillance, dataveillance, biometrics, communications surveillance, sensors and location determination technologies.[628] Further insights into how this typology of surveillance can be used within the PRISMS survey can be found in section 8.2.

[626] TNS Opinion and Social, 2011, p.64.
[627] The Gallup Organization, 2008, pp. 135-136.
[628] Bellanova, et al., 2012.

From the analysis of surveys, partners have found that the operationalisation of the term "surveillance" is often conducted in such a way as to either provide respondents with an example of a form of surveillance technology or, by defining the term in the context of the recording of behaviour or the investigation of individuals. Partners have also identified ways in which public attitudes towards surveillance are measured: predominantly with the use of closed questions in the form of a Likert scale or simply by providing individuals with a choice in relation to preference. In both instances, participants are provided with a neutral option from which to choose, and are therefore not forced to select an answer that may not be applicable to their attitudes.

By investigating the operationalisation of concepts surrounding the issues of privacy, trust, security and surveillance, partners are able to provide a series of recommendations for future surveys. In particular, in the following section, partners provide recommendations for the PRISMS survey.

8.2 RECOMMENDATIONS FOR THE PRISMS SURVEY

Careful wording of questions is essential to achieve useful and reliable survey data. This section briefly highlights examples of "good practice" in question construction that could be useful for the PRISMS survey.

Prior to identifying these hypothesis and potential questions to respond to them, survey designers should consider the various aspects of survey question design that could influence the validity and reliability of their survey. Bryman provides rules to be taken into consideration by questionnaire designers. First, on a general level, Bryman advises researchers to consider their research questions and what they want to find out. Researchers should ensure that the questions in their survey are clear and that, essentially, whether there are any there are any other goals that should be kept in mind in the design stages. Second, Bryman outlines mistakes to be avoided in the design of a survey:[629]

- avoid ambiguous terms in questions (e.g., "often" and "regularly"),
- avoid long questions,
- avoid double-barrelled questions (questions that ask about two things),
- avoid general questions[630],
- avoid leading questions,
- avoid questions that include negatives and
- avoid technical terms.

In addition to these recommendations, Judd et al. emphasise the importance of researchers' using specific questions when trying to understand public attitudes so as to ensure that researchers gain valid responses from participants, rather than general ones.[631] The recommendations by Bryman and Judd et al. provide useful guidelines for the PRISMS survey, and have been useful in assessing survey questions used elsewhere that could inform the PRISMS survey. As a result of the efforts by partners in PRISMS Task 7.1, via this report,

[629] Bryman, 2008, pp. 240-243.
[630] Within the construction of the PRISMS survey, it could be beneficial to ask general questions about issues surrounding privacy and security (for instance) before going into greater detail; however it is important to not rely solely on "general" questions.
[631] Judd et al., 1991, p. 232.

we are able to offer five general observations and recommendations as portrayed in the figure below:

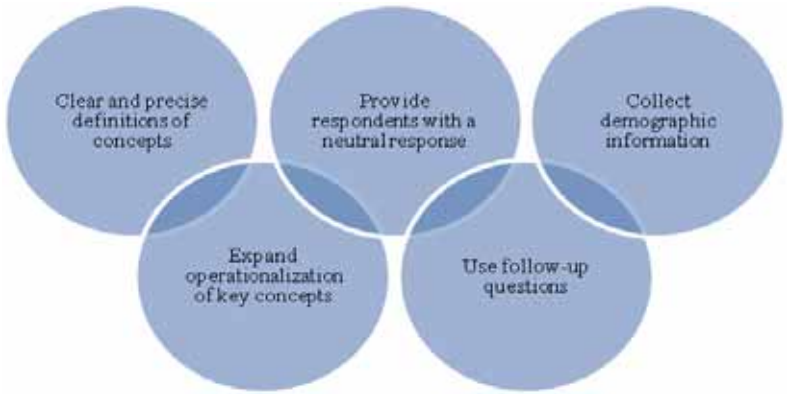


Figure 46: Recommendations for PRISMS survey

First, surveys should offer respondents adequate, clear and precise definitions of the concepts that they are investigating. Second, researchers should avoid limiting the operationalisation of their concepts to narrow individual types of privacy, security and surveillance, and should avoid relying on questions relating these concepts to personal data. Third, future surveys should include (where possible) follow-up questions to attempt to understand respondents' reasoning behind their answers and, finally, surveys should collect appropriate demographic information to enable comparisons.

The partners' analysis of surveys in PRISMS Task 7.1 revealed a series of potential relationships in need of further exploration. Accordingly, prior to recommending specific questions informed by other surveys, partners have developed a series of hypothesis that can be used in developing the PRISMS survey and help reveal public attitudes towards the complex relationship between privacy, trust, security and surveillance. Whilst there are numerous avenues of enquiry, in order to fulfil the goals of PRISMS, the PRISMS survey should focus on responses to the following hypotheses.

Hypothesis 1: Demographic variables have an impact on public perceptions of privacy, trust, security and surveillance.

The PRISMS survey should ensure that it collects enough demographic data to enable meaningful comparisons between different groups of people in society. The analysis in Task 7.1 demonstrated that categories such as age, gender and education background are particularly useful. Collecting this information as precisely as possible, as attempted in the *Flash Eurobarometer 225: Citizens perceptions of data protection* as well as other Eurobarometers, is ideal:[632]

> Gender [DO NOT ASK - MARK APPROPRIATE]
> [1] Male
> [2] Female
>
> How old are you?

[632] Ibid., p.136.

[_][_] years old
[0 0] [REFUSAL/NO ANSWER]

How old were you when you stopped full-time education?
[Write in THE AGE WHEN EDUCATION WAS TERMINATED]
[_][_] years old
[00] [STILL IN FULL TIME EDUCATION]
[0 1] [NEVER BEEN IN FULL TIME EDUCATION]
[99] [REFUSAL/NO ANSWER]

Although recording precise answers, such as exact age, is not the most efficient way to collect data, it does yield the most useful results for nuanced comparison across a range of social categories.

Hypothesis 2: People have different levels of concern about different types of privacy.

The surveys included in PRISMS Task 7.1 often did not offer respondents adequate or precise definitions of the concepts they were querying, and relied upon an assumption that respondents shared "common sense" definitions. Additionally, as discussed in section 5.1.1, the concept "privacy" has been operationalised, most commonly, by referring to privacy in the form of data and images, which in part, neglects six other types of privacy that merit examination. Accordingly, the PRISMS survey should attempt to understand how concerned people are about different types of privacy (as identified by Finn, Wright and Friedewald) and should also provide respondents with examples to help explain what is meant by these different types of privacy and thus not rely on overly-complex terms. For instance:

> Please indicate whether for the following types of privacy you are very, somewhat, not very or not at all concerned. If unsure, please select "don't know".

	Very concerned	Somewhat concerned	Not very concerned	Not at all concerned	Don't know
Privacy of personal data and images (e.g., sharing of personal data such as your mobile number when purchasing a product online.[633])					
Privacy of the person (e.g., the use of a full-body scanner at an airport.[634])					
Privacy of behaviour and action (e.g., the use of CCTV cameras to record your behaviour.[635])					

[633] Partly based on the wording of a question in: TNS Opinion and Social, 2011, p. 16 (Questionnaire).
[634] Partly based on the wording of a question in: Unisys Security Index, 2012, p. 24.
[635] Partly based on the wording of a question in: TNS Opinion and Social, 2011, p.64.

	Very concerned	Somewhat concerned	Not very concerned	Not at all concerned	Don't know
Privacy of communication (e.g., the interception of your e-mail by law enforcement agencies.)					
Privacy of location and space (e.g., the use of mobile phone signals to track your movements or identify your location.)					
Privacy of thoughts and feelings (e.g., the use of specialist equipment in a shop to monitor how interested you are in different products.)					
Privacy of association (e.g., monitoring the groups to which you belong)					

Hypothesis 3: Different explanations are important to people in determining their acceptance of encroachments upon their privacy.

Of utmost important to PRISMS is for partners to be able to understand how people come to understand encroachments upon their privacy. Accordingly, the PRISMS survey should consider the various attributes that may lead to individuals accepting a loss of privacy in their lives, particularly examining the trade-off between privacy and security. Possible areas of enquiry include:

- Acceptance of encroachments upon privacy as "being part of everyday life".[636]
- Encroachments upon privacy to enhance different types of security:[637]
  - Physical security
  - Political security
  - Socio-economic security
  - Cultural security
  - Environmental security
  - Radical uncertainty security
  - Cyber security

[636] As examined by TNS Opinion and Social, 2011.
[637] Lagazio, M., 2012.

Hypothesis 4: Citizens only take some measures of which they are aware to protect their privacy.

In order to further understand how individuals choose to protect their privacy, we should consider the different measures available to them to protect different types of privacy (e.g., privacy of thoughts and feelings and privacy of data). Accordingly, partners involved in designing the PRISMS survey could ask scenario-based questions in relation to knowledge and/or use of available measures and different types of privacy. For instance, as used by the *PEW Internet & American Life Project: Digital Footprints* project, partners could formulate a scenario involving a social network (e.g., Facebook) and ask about measures people could take to protect their privacy.

> When using a social networking account (e.g., Facebook or LinkedIn), are you aware of the following measures, and do you use them? (Please indicate yes or no).

Measure	**Are you aware of this measure?**	**Do you use this measure?**
Amend privacy settings		
Avoid disclosing personal information		
Avoid sharing photographs		
Avoid sharing videos		
Avoid linking your apps (e.g., games) to your account		
Avoid sharing personal information (e.g., date of birth)		
Close your account		

A second type of scenario could be based on the purchasing of goods. For instance:

> When planning to purchase an item (e.g., a book) on the Internet, would you do any of the following?

Measure[638]	**Yes**	**No**	**Maybe**
Provide false information			
Refuse to provide information			
Ask for personal information to be removed			
Read the privacy policy			
Ask a company not to sell information			
Ask that you be removed from the company's marketing list			
Avoid disclosing payment details online (not buy the item)			

By using scenario-based questions, partners will be able to further understand public actions in relation to specific (realistic) examples. In both cases, researchers should understand why some people choose not to take available measures. Accordingly, researchers should use a follow-up question to gain further insights into people's behaviour. An example (leading on from the purchase question above) could be:

> Please indicate why you decided not to take this measure:
> - I was not aware of this an option.

[638] This list of measures was taken from those surveys assessed in PRISMS 7.1 – Section 3.3.3.

- It was too time-consuming.
- I did not feel comfortable doing so. *(Here it may be useful to have an open question to ask why this was the case).*
- I do not think this is an issue, and therefore choose not to take any action.
- Other *(Here it may, again, be useful to have an open question to ask for the respondent to specify)*

Hypothesis 5: Citizens have different levels of trust in different organisations' abilities or willingness to ensure their different types of privacy.

In order to understand the complex relationship between trust and privacy, partners should use the PRISMS survey to try to understand trust in relation to different types of organisations and different types of privacy. Those designing the survey should define trust, and not assume that respondents know what it is meant by the term. The following type of question could be used to further understand the relationship between privacy and trust.

> Please indicate the level of trust you have towards the following organisations in relation to the various types of privacy listed: (Please select from: "totally trust", "tend to trust", "tend not to trust", "do not trust at all" and "Don't know"[639]). "Trust", in this question, refers to the confidence that one has in someone to guarantee and ensure the safety of their privacy.[640]

	Private organisations (e.g., places where you shop, banks, etc.)[641]	**Public organisations (e.g., police, government, etc.)**
Privacy of data and image (e.g., date of birth, address, marital status)		
Privacy of communication (e.g., phone or e-mail records/conversations)		
Privacy of the person (e.g., biometric data such as finger prints, signature)		
Privacy of thoughts and feelings (e.g., the use of specialist equipment on the Internet to monitor how interested you are in different products)		
Privacy of behaviour and action (e.g., religious practices)		
Privacy of location and space (e.g., monitoring where you go in your vehicle)		
Privacy of association (e.g., monitoring the groups of people – trade unions, political parties, religious groups with whom you associate)		

[639] Options taken from: TNS Opinion and Social, 2011, p. 17 (Appendix - Questionnaire).
[640] Note: Within the PRISMS survey it will be necessary to confirm, among partners, how the concept of "trust" is addressed.
[641] Taken from: Greenville et al., 2010, p. 74.

If desired, partners could segment the types of organisations into narrower categories as conducted in the *Flash Eurobarometer 225: Data Protection in the European Union: Citizens' Perceptions,* however it would be necessary to consider the length of the questionnaire and the amount of time that the questionnaire is intended to take up so as to avoid over burdening respondents.[642]

- Medical services and doctors
- Police
- Social security
- Tax authorities
- Local authorities
- Banks and financial institutes
- Employers
- Insurance companies
- Credit card companies
- Non-profit organisations
- Credit reference agencies
- Market and opinion research companies
- Travel companies
- Mail order companies

Hypothesis 6: Citizens hold different levels of concern over different types of security.

As discussed in section 5.1.3, researchers have operationalised the concept "security", most commonly, by referring to physical security and cyber security, which neglects other types of security that also merit examination. Accordingly, the PRISMS survey should attempt to understand whether people are concerned about different types of security, which would help partners to understand what types of security are important to people. Partners could use a strategy similar to that regarding understanding public attitudes towards different types of privacy, where a closed question asks the respondent to select (from a list) different scenarios (based on the seven types of security identified by Lagazio) that show, based on a Likert scale, the extent of their concern. For instance:

> Please indicate how concerned you are about the following different types of security [Please select from the following options: Very concerned, somewhat concerned, not very concerned, not at all concerned, don't know]

	Very concerned	**Somewhat concerned**	**Not very concerned**	**Not at all concerned**	**Don't know**
Physical security (e.g., protection from being burgled).					
Political security (e.g., protection of own rights)					
Socio-economic security (e.g., protection of future employment)					

[642] The Gallup Organization, 2008, p. 10.

	Very concerned	Somewhat concerned	Not very concerned	Not at all concerned	Don't know
Cultural security (e.g., protection of values and morals)					
Environmental security (e.g., protection of access to and safe use of natural resources)					
Radical uncertainty security (e.g., protection from sudden emergencies)					
Cyber security (e.g., safe access on the Internet)					

Hypothesis 7: Citizens are more concerned about the impact of some surveillance technologies on their privacy than others.

In order to respond to this hypothesis, partners should distinguish between different types of surveillance technologies as identified by Bellanova et al.[643], and how they may impact upon different types of privacy. Accordingly, partners may be able to use the following question:

> Please indicate how concerned you are about the impact of the following types of surveillance technologies upon your privacy (e.g., private/personal life):

	Very concerned	Somewhat concerned	Not very concerned	Not at all concerned	Don't know
Visual surveillance (e.g., CCTV)					
Dataveillance (e.g., monitoring of financial transactions)					
Biometrics (e.g., storing of finger prints)					
Communication surveillance (e.g., monitoring of telephone calls)					

[643] Bellanova et al. (2012).

	Very concerned	Somewhat concerned	Not very concerned	Not at all concerned	Don't know
Location determining technologies (e.g., GPS tracking)					
Sensor technologies (e.g., infrared camera)					

The question above caters for understanding citizen concerns in relation to surveillance technologies and how they may affect a person's privacy. Such a question naturally lends itself to asking further questions about surveillance technologies – in relation to trust and security (see hypothesis 8a, b and c below).

Hypothesis 8a: Citizens have different beliefs in the ability of different types of surveillance technologies to enhance security.

Hypothesis 8b: Citizens are concerned about different types of surveillance technologies and their impact on their privacy.

Hypothesis 8c: Citizens have different levels of trust in an authority's abilities to protect their privacy when using surveillance technologies to enhance security.

In addition to understanding public attitudes towards surveillance technologies and their impact on their privacy, partners should use the PRISMS survey to further understand the complex relationship between privacy, trust, security and surveillance. In this case, to account for different types of technologies, privacy, trust and security, partners may need to use several scenarios to gather public attitudes towards these issues.

The following scenario provides an example:

1. **Scenario 1: Use of biometric surveillance technologies to enhance physical security and reduce uncertainty at an airport.**
   A. Do you think the use of body scanners at an airport can enhance physical security against an attempted plane hijacking?
      a. Yes
      b. No
      c. Don't know

   B. Do you think a body scanner infringes upon your privacy (e.g., personal privacy)?
      a. Strongly agree
      b. Somewhat agree
      c. Somewhat disagree
      d. Strongly disagree
      e. Neither agree nor disagree

C. Do you trust authorities (e.g., border staff) to protect your privacy (e.g., by not retaining your image) in relation to the use of a body scanner?[644]
    a. Totally trust
    b. Tend to trust
    c. Tend not to trust
    d. Do not trust at all
    e. Don't know

D. If you answered "c" or "d" to question C, why do you feel this way?
    a. This is an invasion of my privacy
    b. I do not trust that authorities will protect details
    c. I feel the authorities may misuse my details
    d. Other
    e. Don't know

In this scenario, partners should ask some follow-up questions to fully understand the complex relationship surrounding all four issues. Additional scenarios, such as those being developed in PRISMS WP2, could be used to address different types of privacy and surveillance technologies. Such a technique has the potential to further our understanding of public attitudes towards the trade-off between privacy and security, allowing for opinions towards trust and surveillance to be understood at the same time.

8.3 CONCLUSION

Following PRISMS Tasks 7.1 and 7.3, partners have been able to provide a series of recommendations in relation to hypotheses and questions that can be used in future surveys relating to privacy, trust, security and surveillance. Future surveys, such as that in PRISMS, should make an effort to ensure that the concepts referenced in their questions are operationalised in such a way as to offer respondents a clear and concise understanding of their meaning. Researchers should not assume that respondents will understand the terms they employ. Furthermore, researchers should avoid limiting the operationalisation of their concepts to narrow fields of privacy, security and surveillance. Researchers may also want to open their surveys up by using questions that seek to understand why public attitudes are what they are. Additionally, researchers should include a neutral option to avoid forcing respondents to provide false information; this will assist in enhancing the validity of the survey. As a final point, designers of future surveys should ensure they include socio-demographic questions within their survey so as to be able to compare and contrast results against different social groups.

[644] As trust has been defined in a previous question, it would not be necessary to repeat this step.

Chapter 9: Conclusion: Summary of recommendations

Hayley Watson, David Wright and Rachel Finn
Trilateral Research & Consulting, LLP

9 CONCLUSION: SUMMARY OF RECOMMENDATIONS

The purpose of work package seven of the PRISMS project was to provide an analysis of existing surveys on privacy, security, surveillance and trust with an evaluative component involving the assessment of their reliability, shortfalls and applicability for policy-makers. The work carried out in this work package serves the purpose of contributing to the development of the PRISMS survey in work package nine. The work package consisted of five tasks: an analysis of existing surveys, a meta-analysis of existing surveys, a review of survey questioning techniques, an exploration of shortcomings, lessons learned and longitudinal comparisons, and an analysis of social value surveys. The results of these different tasks have been included in this report.

In this last chapter, we have collated and now present the recommendations from the preceding chapters. For the readers convenience, the recommendations have been organised according to the chapter from which they have been extracted.

Chapter 3: Meta-analysis
The aim of Task 7.2, reported in chapter three, was to take stock of existing surveys at the intersection of surveillance and privacy, to consider them from a methodological standpoint of good practice, to evaluate their reliability and comparability, and to draw lessons from this exercise. This permits an assessment of the quality of surveys, enabling PRISMS to make recommendations regarding methodological considerations for conducting its own survey. The following recommendations were made to be considered during the development of the PRISMS survey:

- The size and range of the PRISMS survey should be directly comparable to the Eurobarometer surveys of privacy-related topics conducted in all the countries of the EU.

- The survey should include contextual and personal questions (also identified in chapter 6, 7 and 8) relating to the daily lives of respondents that could influence their responses.

Chapter 5: Horizontal analysis
The aim of the horizontal analysis of findings from chapter 5 was to provide a horizontal analysis of public attitudes towards the four themes under investigation: privacy, trust, security and surveillance. As a result of this analysis, partners have made the following recommendations that are of direct relevance to the development of the PRISMS survey. The recommendations made in chapter eight were further developed in the recommendation of questions and hypotheses in Task 7.3 (Chapter eight of this report).

- Future research needs to explore all seven types of privacy, and researchers should try to ask why respondents are or are not concerned with different types of privacy. Future research may also want to determine the different measures people use to protect their online privacy including asking respondents how successful they feel they are in maintaining and managing their privacy.

- Future surveys should try to understand whether trust of organisations has any impact on public attitudes towards forgoing privacy to enhance security. Future surveys ought to try and develop questions that seek to further understand why individuals do not trust certain organisations, and what they feel can be done to improve their trust. Surveys should also

try to understand how trusting individuals are of different surveillance technologies and those who operate them.

- Future research ought to try to develop a more comprehensive understanding of the various measures people are choosing to take, or avoiding to take and, crucially, why they are making these decisions.

- Future research must continue to try to understand the relationship between public perceptions of different types of surveillance technologies and what this implies for people's sense of privacy.

Chapter 6: Short comings, lessons learned and longitudinal analysis
The aim of Task 7.4 (reported in chapter six) was to consider any shortcomings or limitations of existing surveys that may provide lessons for the design of the PRISMS survey. Partners have noted extraneous and situational factors that may influence responses, including media portrayals, cultural differences, knowledge of privacy laws and specific events, this was similarly identified in chapter seven when considering the approach of social values surveys to exploring public opinion towards these issues. As a result, partners have formulated a series of hypothesis to be taken into consideration in the development of the PRISMS survey:

- Characteristics of the respondents' personal life history have a significant correlation with the respondents' opinion on, and attitudes towards, privacy, security, trust and surveillance. This correlation is particularly strong in the case of circumstances and experiences in the early stages of the respondents' life (childhood, family life, school) but also traceable in adult age. Naturally, we expect to find correlations between certain demographic data and the circumstances of the respondents' personal life history (for example, higher income – more chance to have a separate room) but we believe that such demographic data cannot fully explain the opinions and attitudes of the respondents, with special regard to individual (bad and good) experience.

- The existence and characteristics of religious or philosophical beliefs (including the characteristics of the religion or church in question) show correlations with the respondents' opinion on, and attitudes towards, privacy, security, trust and surveillance.

- Belonging to ethnic, religious, cultural, sexual or other minorities in society also have a measurable impact on people's view on the borderlines of private and public life. Similarly, other sensitive personal data (health status, pathological addictions, sexual preferences, criminal convictions etc.) may also show correlations with the distribution of survey data. These correlations are bi-directional: belonging to a minority group, or having an illness do not necessarily result in a higher sensitivity to privacy.

- Not only online communication habits but also offline communication experience, including participation in social events, exchange of news and information, the nature of information shared with others, and the expectations of what should and what should not be divulged about the respondent's private life in the various social circles, show correlations with the respondents' views on privacy and related subject areas.

Chapter 7: Analysis of social value surveys
The aim of Task 7.5 (reported in chapter seven) was to understand how social values could be incorporated into the PRISMS survey as wider cultural factors, such as social values are

central to understanding an external indicator capable of influencing public perceptions of privacy, security and related concepts. Consequently, the following hypotheses have been identified:

- The higher the socio economic status of a citizen, the more important privacy is.
- The economic development of a country determines citizen's perceived need for security mechanisms.
- Security is always important, but the focus is different dependent on the higher the income.
- The religion of a citizen influences an individual's perception of privacy
- In those parts of Europe where interpersonal trust is low, citizens are willing to give up privacy for a potential increase in security.

Chapter 8: Recommended questions

The aim of Task 7.3 (reported in chapter eight) was to review and analyse survey question techniques and provide a set of hypothesis and related questions to support the construction of the PRISMS survey. Accordingly, the following recommendations and hypotheses have been outlined for consideration in the development of the PRISMS survey:

- Partners identified general recommendations to be considered in the PRISM survey:
    1. The use of clear and precise definitions of concepts.
    2. Provide respondents with neutral responses to choose from.
    3. Collect demographic information.
    4. Expand the operationalization of key concepts.
    5. Use follow-up questions.

- Partners also identified a set of eight hypothesis (as well as examples of questions) for the PRISMS survey:
    1. Demographic variables have an impact on public perceptions of privacy, trust, security and surveillance.
    2. People have different levels of concern about different types of privacy.
    3. Different explanations are important to people in determining their acceptance of encroachments upon their privacy.
    4. Citizens only take some measures of which they are aware to protect their privacy.
    5. Citizens have different levels of trust in different organisations' abilities or willingness to ensure their different types of privacy.
    6. Citizens hold different levels of concern over different types of security.
    7. Citizens are more concerned about the impact of some surveillance technologies on their privacy than others.
    8. Consists of three parts:
        a) Citizens have different beliefs in the ability of different types of surveillance technologies to enhance security.
        b) Citizens are concerned about different types of surveillance technologies and their impact on their privacy.
        c) Citizens have different levels of trust in an authority's abilities to protect their privacy when using surveillance technologies to enhance security.

ANNEX 1: MAIN CHARACTERISTICS OF THE SURVEYS ANALYSED

ID	Title of survey	Subject area	Who conducted the survey	Client	Date	Surveyed population	Sample size	Method
33	Information Technology and Data Privacy - Eurobarometer 46.1	Europeans' interest in information technology, and concerns regarding their data privacy	INRA (Europe) - E.C.O. (overseeing different polling orgs in Member States)	European Commission DG Internal Market & Financial Services	1996 Oct - Nov	Age 15+ in all 15 Member States of the EU (E/W Germany, N. Ireland separately)	Total: 16,246; min. 1000 per country (Lux. 610, Northern Ireland 324)	Multi-stage cluster sampling, face-to-face in people's homes; in their national language
250	Special 9/11 Poll – Harris Interactive	Public support for law enforcement and surveillance measures in the aftermath of the attacks	Harris Interactive		2002 Aug - Sep	USA	2,203	Online survey
63	A two-edged sword – public attitudes towards video surveillance in Helsinki	Public attitudes towards increasing video surveillance; public perceptions of security	The City of Helsinki Urban Facts		2003 August	Helsinki citizens, age 16-69, random sample	1,240	Mail survey
77.../ 135	URBANEYE: CCTV in Europe	Public attitudes towards CCTV	Centre for Technology and Society, Technical University Berlin (with research partners)	European Commission (a research project under the FP5 Framework Programme)	2004 June - Oct	Berlin, Budapest, London, Oslo and Vienna	5,005	Questionnaire-based street survey

ID	Title of survey	Subject area	Who conducted the survey	Client	Date	Surveyed population	Sample size	Method
101	e-Identity: European attitudes towards biometrics	Public opinion towards the introduction of biometric technology in Europe, and future products relating to identity and financial security	Vanson Bourne (independent research company)	Logica CMG	2006 April	UK, France, Germany, Netherlands, Spain, Czech Republic, Portugal	500	
54	A survey on EU Citizens' Trust in ID Systems and Authorities	Europeans' attitudes towards ID systems and trust in authorities that manage and implement these systems	London School of Economics	European Commission (part of the research project FIDIS under the FP6 Framework Programme)	2006 June	23 EU countries	Unclear sample, reduced to 1,907	Online survey
21	Digital Footprints: Online identity management and search in the age of transparency	Attitudes to personal information online and usage.	Princeton Survey Research Associates	Pew Internet & American Life Project	2006 Nov - Dec	USA nationals, age 18+	2,373	Telephone interviews: random digit sample of telephone numbers
34	Globalization of Personal Data	An international survey on privacy and surveillance	Ipsos	Social Sciences and Humanities Research Council of Canada / Queens University	2006-2007	Adults in Canada, USA, France, Spain, Hungary, Mexico, Brazil, China, Japan	9,606	Computer assisted telephone interviews; preliminary focus group discussions

ID	Title of survey	Subject area	Who conducted the survey	Client	Date	Surveyed population	Sample size	Method
5	Data Protection in the European Union: Citizens' perceptions. Flash Eurobarometer 225	Public's general feelings and concerns about data privacy	Gallup Organization Hungary	Directorate-General Justice, Freedom and Security	2008 Jan - Feb	Age 15 + in the 27 EU Member States	Over 27,000	Mainly by fixed-line telephone; in CEE countries face-to-face, too
12	Personlig Integritet: A Comparative Study of Perceptions of Privacy in Public Places in Sweden and the United States	Cross-cultural study of people's judgments about privacy in public places	University of Washington, Stockholm University, Seattle Pacific University		2008 Oct	University campuses in Sweden and USA (mixed age categories)	350 Sweden + 30 interviews; 250 USA + 30 interviews	Self-completion questionnaires plus face-to-face interviews
59	Privacy 2.0: personal and consumer protection in the new media reality	Use of social media and challenges for consumers in relation to their privacy	SINTEF	The Norwegian Consumer Council	2008-2009	Norway, Internet users	1,372	E-mail survey
45	Pew Internet & American Life Project: Reputation Management and Social Media	How people manage their online identity in social media	Princeton Survey Research Associates International	Pew Internet & American Life Project	2009 Aug - Sept	USA, Age 18 +	2,253	Landline and mobile telephone interviews
50	Canadians and Privacy	Public understanding of privacy issues, legislation and federal privacy institutions	EKOS Research Associates Inc.	Office of the Privacy Commissioner of Canada (OPC)	2009 Feb - March	Canadians, random sample, age 18 +	2,028	Telephone survey

ID	Title of survey	Subject area	Who conducted the survey	Client	Date	Surveyed population	Sample size	Method
32	EU Kids Online	Children's use and experiences of the Internet in the EU, with supplementary information from parents	Ipsos MORI	EU Kids Online consortium; London School of Economics	2010 April - Aug	9-16 year old internet users and parents in 25 EU countries	23,420	Face-to-face interviews plus self-completion questionnaires
6	Unisys Security Index	How safe consumers feel on key areas of security	International Communications Research ICR	(Unisys Security Index)	2010 Feb	Age 18+ Australia, Belgium, Brazil, Germany, Mexico, Netherlands, New Zealand, Spain, UK, USA	9,429	Telephone, online and face-to-face
35	Financial Times/Harris Poll: Body Scanners	Public attitudes towards body scanners at airports	Harris Interactive	Financial Times/Harris Poll	2010 Feb	France, Germany, Great Britain, Spain, Italy, USA, China	7,256	Online survey
44	State of the Nation Survey 2010	Public opinion on government policies, and on privacy, surveillance, trust and security	ICM	Joseph Rowntree Reform Trust	2010 Feb	British residents, representative, age 18 +	2,288	Face-to-face in public spaces

ID	Title of survey	Subject area	Who conducted the survey	Client	Date	Surveyed population	Sample size	Method
229	Attitudes on Data Protection and Electronic Identity in the European Union (Special Eurobarometer 359)	Awareness of, and attitudes on disclosure of personal data, profiling, identity management, DP law	TNS Opinion & Social	European Commission: Joint Research Centre (JRC), DG JUST	2010 Nov - Dec	Age 15+ in the 27 EU Member States, representative	Total: 26,574; about 1,000 per country	Face-to-face in people's homes; in their national language
259	Online Profile and Reputation Perceptions Study	Public attitudes towards the creation and consequences of having an online profile	Blueocean Market Intelligence & Telecommunications Research Group	Microsoft	2011 Nov	Three age groups from Canada, Germany, Ireland, Spain, USA	Total: 5000, 1000 per country	
255	Internet Privacy Research	Australian attitudes towards privacy on the Internet	Social Research Centre	University of Queensland Centre for Critical and Cultural Studies (component of the November 2011 Dual Frame Omnibus Survey)	2011 Nov - Dec	Age 18+ in Australia, random sample	1,016	Landline and mobile telephone survey

ANNEX 2: LIST OF 21 "PORTRAIT VALUES QUESTIONNAIRES" (PVQ) ITEMS FOR THE EUROPEAN SOCIAL SURVEY (ESS)

Basic value	Core motivational goal	PVQ items in the ESS
UN: universalism	Understanding, appreciation, tolerance and protection for the and for nature welfare of all people	He thinks it is important that every person in the world should be treated equally. He believes everyone should have equal opportunities in life.
		It is important to him to listen to people who are different from him. Even when he disagrees with them, he still wants to understand them.
		He strongly believes that people should care for nature. Looking after the environment is important to him.
BE: benevolence	Preservation and enhancement of the welfare of people with whom one is in frequent personal contact	It is very important to him to help the people around him. He wants to care for their well-being.
		It is important to him to be loyal to his friends. He wants to devote himself to people close to him.
TR: tradition	Respect, commitment, and acceptance of the customs and ideas that one's culture or religion impose on the individual	It is important to him to be humble and modest. He tries not to draw attention to himself.
		Tradition is important to him. He tries to follow the custom handed down by his religion or his family.
CO: conformity	Restraint of actions, inclinations, and impulses likely to upset or harm others and violate social expectations or norms	He believes that people should do what they are told. He thinks people should follow rules at all times, even when no one is watching.
		It is important to him always to behave properly. He wants to avoid doing anything people would say is wrong.
SE: security	Safety, harmony, and stability of society, of relationships, and of self	It is important to him to live in secure surroundings. He avoids anything that might endanger his safety.
		It is important to him that the government ensures his safety against all threats. He wants the state to be strong so it can defend its citizens.
PO: power	Social status and prestige, control or dominance over people and resources	It is important to him to be rich. He wants to have a lot of money and expensive things.
		It is important to him to get respect from others. He wants people to do what he says.
AC: achievement	Personal success through demonstrating competence according to social standards	It is important to him to show his abilities. He wants people to admire what he does.
		Being very successful is important to him. He hopes people will recognize his achievements.

HE: hedonism	Pleasure and sensuous gratification for oneself	Having a good time is important to him. He likes to "spoil" himself.
		He seeks every chance he can to have fun. It is important to him to do things that give him pleasure.
ST: stimulation	Excitement, novelty, and challenge in life	He likes surprises and is always looking for new things to do. He thinks it is important to do lots of different things in life.
		He looks for adventures and likes to take risks. He wants to have an exciting life.
SD: self-direction	Independent thought and action in choosing, creating, exploring	Thinking up new ideas and being creative is important to him. He likes to do things in his own original way.
		It is important to him to make his own decisions about what he does. He likes to be free and not depend on others.

Source: Schwartz, "A Proposal for Measuring Value Orientations across Nations", 2003.

ANNEX 3: ADDITIONAL HYPOTHESES FROM THE ANALYSIS OF SOCIAL VALUES SURVEYS (CHAPTER 7)

- Individualistic countries care more about privacy, but in terms of individual control and autonomy.
- Individualistic countries tend to give up privacy more easily.
- Non-individualistic countries care about privacy in traditional terms and care less about individual privacy than individualistic countries.
- Eastern countries value personal liberties especially high but also have a tendency that citizens hide away.
- Privacy of the person is more important for citizens from Northern Europe than for citizens from East and Central Europe.
- The higher the emphasis on self-expression values in a country, the more important is privacy.
- Citizens from Western European countries put a stronger emphasis on self-autonomy than people from Eastern and Central European countries.
- Societies that rank high on self-expression values also tend to emphasise interpersonal trust.
- People living in Eastern and Central European countries value security higher than people living in Northern and Western European countries.

ANNEX 4: CLUSTERING OF EUROPEAN COUNTRIES

Based on the work we did, we developed a first cluster of European countries. Nevertheless we have to acknowledge that overlaps exist and a definite categorization is rather difficult. The following grouping is to be understood under reserve.

1	Spain, Italy, Malta, Greece, Cyprus, France?, Portugal
2	Germany, Belgium, Netherlands, Luxemburg, Austria, France?
3	Denmark, Sweden, Finland
4	Latvia, Lithuania, Estonia
5	United Kingdom, Ireland
6	Slovenia, Slovakia, Czech Republic, Hungary
7	Romania, Bulgaria

REFERENCES

Adair, Aly, "Will Your Digital Footprint Cost You a Job and College Admission?", *Yahoo! Voices*, 24 February 2009. http://voices.yahoo.com/will-digital-footprint-cost-job-college-2741408.html?cat=3

Allport, Gordon W., *Personality. A psychological interpretation*, Holt, New York, 1937.

Arnott, Christy, *Internet Privacy Research*, The University of Queensland Australia, February 2012.

Arts, Wil, and Loek Halman, "European value changes in the second age of modernity", in Wil Arts, and Loek Halman (eds.), *European Values at the Turn of the Millennium*, Brill, Leiden, Boston, 2004a.

Arts, Wil, and Loek Halman (eds.), *European Values at the Turn of the Millennium*, Brill, Leiden, Boston, 2004b.

Arts, Wil, and Loek Halman, "European Values at the Turn of the Millennium: An Introduction", in Wil Arts, and Loek Halman (eds.), *European Values at the Turn of the Millennium*, Brill, Leiden, Boston, 2004c.

Backhouse, James, and Ruth Halperin, *D4.5: A Survey on Citizen's Trust in ID Systems and Authorities: Future of IDentity in the Information Society*, Deliverable 4.5 of the FIDIS project, 17 April 2007. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.5.a_survey_on_EU_citizens_trust.pdf

Backhouse, James, and Ruth Halperin, "A Survey on EU Citizens' Trust in ID Systems and Authorities", *FIDIS Journal*, No. 1, June 2007. http://journal.fidis.net/fileadmin/journal/issues/1-2007/Survey_on_Citizen_s_Trust.pdf

Bales, Robert. F., and Arthur. S. Couch, "The value profile: A factor analytic study of value statements", *Sociological Inquiry*, Vol. 39, 1969, pp. 3-17.

Balz, Dan, and Claudia Deane, "Differing Views on Terrorism", *The Washington Post*, 11 January 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/01/10/AR2006011001192.html

Bauman, Zygmunt, *In Search of Politics*, Polity Press, Cambridge, 1999.

Bay, Hans, "European Values Map: Based on ESS data", Paper presented at the *Sixth International Conference on Social Science Methodology*, Amsterdam, 2004.

Gutwirth, Serge, Rocco Bellanova, Michael Friedewald, Dara Hallinan, David Wright, Paul McCarthy, Julien Jeandesboz, Emilio Mordini, Silvia Venier, Marc Langheinrich, and Vlad Coroama, "Smart Surveillance - State of the Art Report", Deliverable 1, SAPIENT Project, 2012. http://www.sapientproject.eu/docs/D1.1-State-of-the-Art-submitted-21-January-2012.pdf

Best, Samuel, J., Brian Krueger S., and Jeffrey Ladewig, "The Polls - Trends. Privacy in the Information Age", *Public Opinion Quarterly*, Vol. 70, No. 3, 2006, pp. 375–401.

Brackenbury, Ian, and Thomas Wong, *Online Profile & Reputation Perceptions Study*, Microsoft Corporation, 2011. http://go.microsoft.com/?linkid=9797356

Brandtzaeg, Petter Bae and Markia Luders, *Privacy 2.0: Personal and Consumer Protection in the New Media Reality*, SINTEF Report, The Norwegian Consumer Council, 2 November 2009. http://sintef.academia.edu/PetterBaeBrandtz%C3%A6g/Papers

Brooks, David J., "What is security: Definition through knowledge categorization", *Security Journal*, Vol. 23, No. 3, 2009, pp. 225-239. http://www.palgrave-journals.com/sj/journal/v23/n3/full/sj200818a.html

Bryman, Alan, *Social Research Methods*, 3rd ed., Oxford University Press, Oxford, 2008.

Bürklin, Wilhelm, Markus Klein, and Achim Ruß, "Dimensionen des Wertewandels: eine empirische Längsschnittanalyse zur Dimensionalität und der Wandlungsdynamik gesellschaftlicher Wertorientierungen", *Politische Vierteljahresschrift*, Vol. 35, No. 4, 1994, pp. 579- 606.

Case, Amy, "Digital Footprint", Blog, *Cyborg Anthropology*, 23 October 2010. http://cyborganthropology.com/Digital_Footprint

Clarke, Roger, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", Xamax Consultancy, August 1997. http://www.rogerclarke.com/DV/Intro.html

Davis, Darren, and Brian Silver, "Americans Protect Civil Liberties", *Institute for Public Policy and Social Research Policy Brief*, Vol. 4, April 2002. http://ippsr.msu.edu/Documents/PolicyBrief/911Briefing.pdf

Davison, Robert M., Roger Clarke, H. Jeff Smith, Duncan Langford and Bob Kuo, “Information Privacy in a Globally Networked Society: Implications for IS Research”, *Communication of the Association for Information Systems*, Vo. 12, 2003, pp. 341-365.

De Hert, Paul, and Serge Gutwirth, "Regulating Profiling in a Democratic Constitutional State", in Mireille Hildebrandtand Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008, pp. 271-291.

Deisman, Wade, Patrick Derby, Aaron Doyle, Stephane Leman-Langlois, Randy Lippert, David Lyon, Jason Pridmore, Emily Smith, Kevin Walby and Jennifer Whitson, *A Report on Camera Surveillance in Canada: The Surveillance Project*, Surveillance Camera Awareness Network (SCAN), 30 January 2009.http://qspace.library.queensu.ca/bitstream/1974/1906/1/SCAN_Report_Phase1_Final_Jan_30_2009.pdf

van Deth, Jan W., and Elinor Scarbrough, "The Concept of Values", in Jan W. van Deth, and Elinor Scarbrough (eds.), *The Impact of Values*, Oxford University Press, Oxford, 1995, pp. 21-47.

Dillman, Don A., “The Design and Administration of Mail Surveys”, *Annual Review of Sociology*, Vol. 17, 1991, pp. 225-249.

EKOS Research Associated Inc., *Canadians and Privacy: Final Report*, March 2009. http://www.priv.gc.ca/information/por-rop/2009/ekos_2009_01_e.asp

ESRAB (European Security Research Advisory Board), "Meeting the challenge: the European Security Research Agenda. A report from the European Security Research Advisory Board", Office for Official Publications of the European Communities, Luxembourg, 2006. http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf

European Commission, "Overview of information management in the area of freedom, security and justice", COM(2010) 385 final, Brussels, 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0385:FIN:EN:PDF

European Commission, “Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)”, COM(2012) 11 final, Brussels, 25 January 2012. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

European Commission, “Why Do We Need an EU Data Protection Reform?”, 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT

European Council, The Stockholm Programme – An open and secure Europe serving and protecting the citizens, 17024/09, Brussels, 2 Dec 2009 and European Commission, “An area of freedom, security and justice serving the citizen”, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, COM(2009) 262 final, Brussels, 2009.

European Parliament and the Council, Directive 95/94/EC, of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal*, L 281, 23 November 1995. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

European Social Survey, "ESS Source Questionnaire Final (Round 5, 2010/11)", 2010.

European Urban Knowledge Network, “EUKN - ‘A Two-edged Sword’ - a Research on the Attitudes of Helsinki Citizens Toward Video Surveillance”, 16 October 2003. http://www.eukn.org/E_library/Security_Crime_Prevention/Crime_Prevention/Camera_Surveillance/A_two_edged_sword_a_research_on_the_attitudes_of_Helsinki_citizens_toward_video_surveillance

European Values Study, "EVS 2008 Master Questionnaire. Related to the Integrated Dataset Archive-Study-No. ZA4800, DOI:10.4232/1.10059", GESIS - Leibniz-Institut für Sozialwissenschaften, Mannheim, 2008.

Finn, Rachel L., David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Yves Poullet et al. (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, pp. 3-32.

Flanagan, S., and A. R. Lee, "The new politics, culture wars, and the authoritarian-libertarian value change in advanced industrial democracies", *Comparative Political Studies*, Vol. 36, 2003, pp. 235-270.

Friedman, Batya, Kristina Hook, Brian Gill, Lina Eidmar, Catherine Sallmander Prien and Rachel Severson, "Personlig Integritet: A Comparative Study of Perceptions of Privacy in Public Spaces in Sweden and the United States", *5th NordiCHI*, Sweden, 2008, pp. 142–151. http://dl.acm.org/citation.cfm?doid=1463160.1463176

Friedewald, Michael (editor), *Central Concepts and Implementation Plan,* Deliverable 1.1 of the PRISMS project, 29 March 2012.

The Gallup Organization, *Data Protection in the European Union: Citizens' Perceptions - Analytical Report*, Flash Eurobarometer Series #225, March 2008. http://ec.europa.eu/public_opinion/archives/flash_arch_239_225_en.htm

Gandy, Oscar H., Jr, "Public Opinion Surveys and the Formation of Privacy Policy", *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 283-299.

Gill, Martin, Jane Bryan and Jenna Allen, "Public Perceptions of CCTV in Residential Areas", *International Criminal Justice Review*, Vol. 17, No. 4, 1 December 2007, pp. 304-324.

Grenville, Andrew, "Shunning Surveillance or Welcoming the Watcher? Exploring How People Traverse the Path of Resistance", in Elia Zurelik, Lynda L. Harling Stalker, Emily Smith, David Lyon and Yolande E. Chan (eds.), *Surveillance, Privacy and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal and Kingston, 2010, pp. 70–83.

Groves, R.M., R.B. Cialdini and M.P. Couper, "Understanding the Decision to Participate in a Survey", *Public Opinion Quarterly*, Vol. 56, 1992, pp. 475-495.

Gutwirth, Serge, *Privacy and the Information Age*, Rowman & Littlefield, Lanham, MA, 2002.

GVU Center, *GVU's 8th WWW Survey Results*, GVU's WWW User Surveys, College of Computing, Georgia Institute of Technology, 1997. http://www.cc.gatech.edu/gvu/user_surveys/survey-1997-10/#exec

Hagenaars, Jacques, Halman, Loek, Moors, Guy, "Exploring Europes's basic value map", in Arts, Wil, Hagenaars, Jacques and Halman, Loek, (eds.), *The cultural diversity of European Unity. Findings, Explanations and Reflections form the European Values Study*, 2003, pp. 23-49.

Haggerty, Kevin D. and Amber Gazso, "The Public Politics of Opinion Research on Surveillance and Privacy", *Surveillance & Society*, Vol. 3, Nos. 2-3, 2005, pp. 173-180.

Halman, Loek, Inge Sieben, and Marga van Zundert, *Atlas of European Values. Trends and Traditions at the turn of the Century*, Brill, Leiden, 2012.

Harris Interactive, *Overwhelming Public Support for Increasing Surveillance Powers and, Despite Concerns About Potential Abuse, Confidence That the Powers Will Be Used Properly*, 3 October 2001. http://www.harrisinteractive.com/NEWS/allnewsbydate.asp?NewsID=370

Harris Interactive, "Most People Are 'Privacy Pragmatists' Who, While Concerned About Privacy, Will Sometimes Trade It Off for Other Benefits, Says Harris Interactive Survey", *The Free Library*, 19 March 2003. http://www.thefreelibrary.com/_/print/PrintArticle.aspx?id=98931112

Harris Interactive, *Most Adults in Largest European Countries, U.S. and China Agree Full Body Scanners Should Be Introduced in Airports*, 3 March 2010. http://www.harrisinteractive.com/vault/HI_FinancialTimes_HarrisPoll_March_2010_02.pdf

Harris, Louis and Alan F. Westin, *Harris-Equifax Consumer Privacy Survey 1991*, Equifax, Atlanta, 1991.

Hillmann, Karl-Heinz, "Zur Wertewandelforschung: Einführung, Übersicht und Ausblick", in Georg W. Oesterdiekhoff, and Norbert Jegelka (eds.), *Werte und Wertewandel in westlichen Gesellschaften, Resultate und Perspektiven der Sozialwissenschaften*, Leske and Budrich, Opladen, 2001, pp. 15-39.

Hixson, Richard F., *Privacy in a public society. Human rights in conflict*, New York, Oxford University Press, 1987.

Hofstede, Geert, *Culture's Consequences – Comparing Values, Behaviors, Institutions and Organizations Across Nations*, Sage, London, 2001.

Hofstede, Geert, and Gert Jan Hofstede, *Lokales Denken, globales Handeln. Interkulturelle Zusammenarbeit und globales Management*, Deutscher Taschenbuch Verlag, München, 2009.

Hempel, Leon, and Eric Topfer, *URBANEYE: CCTV in Europe*, Centre for Technology and Society, Technical University Berlin, August 2004. http://www.URBANEYE.net/results/ue_wp15.pdf

Hoofnagle, Chris, Jennifer King, Su Li and Joseph Turrow, "How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?", *Social Science Research Network*, 14 April 2010. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864

Horrigan, John B., *Use of Cloud Computing Applications and Services*, Data Memo, PEW Internet & American Life Project, September 2008. http://www.pewinternet.org/~/media/Files/Reports/2008/PIP_Cloud.Memo.pdf

House of Commons Home Affairs Select Committee, *A Surveillance Society?*, Fifth Report of Session 2009-10, HC 58-I, The Stationery Office, London, 8 June 2008.

House of Lords, Select Committee on the Constitution, 2nd Report of Session 2008-09, *Surveillance: Citizens and the Tate*, Volume I: Report, HL Paper 18-I, paras. 399, 400.

Hudson, John, "Institutional Trust and Subjective Well-Being across the EU", in *Kyklos,* Vol. 59, No. 1, 2006, pp. 43–62.

Inglehart, Ronald, *The Silent Revolution: Changing Values and Political Styles among Western Publics*, Princeton University Press, Princeton, 1977.

Inglehart, Ronald, *Modernisierung und Postmodernisierung. Kultureller, wirtschaftlicher und politischer Wandel in 43 Gesellschaften*, Campus, Frankfurt/Main, 1998.

Inglehart, Ronald, and Christian Welzel, *Modernization, Cultural Change and Democracy*, Cambridge University Press, New York, Cambridge, 2005.

Inglehart, Ronald, "Mapping Global Values", in Yilmaz Esmer, and Thorleif Pettersson (eds.), *Measuring and Mapping Cultures: 25 Years of Comparative Value Surveys*, Brill, Leiden, Boston, 2007, pp. 11-32.

INRA (Europe), *Eurobarometer 46.1: Information Technology and Data Privacy*, European Commission, January 1997. http://ec.europa.eu/public_opinion/archives/ebs/ebs_109_en.pdf

The Joseph Rowntree Reform Trust Ltd. and ICM, *State of the Nation 2010 Poll*, 20 March 2010. http://www.jrrt.org.uk/publications/state-nation-2010-poll

Judd, Charles M., R. Eliot Smith and Louise H. Kidder, *Research Methods in Social Relations*, 6th ed., Holt, Rinehart & Winston, London, 1991.

Katz, James, E., and Annette Tassone R., "The Polls - a report. Public Opinion Trends: Privacy and Information Technology", *Public Opinion Quarterly*, Vol. 54, 1990, pp. 125–143.

Klages, Helmut, "Die gegenwärtige Situation der Wert- und Wertewandelsforschung - Probleme und Perspektiven", in Helmut Klages, Hans-Jürgen Hippler et al. (eds.), *Werte und Wandel*, Campus, Frankfurt/Main, 1992, pp. 5-39.

Klages, Helmut, and Herbert, Willi, *Wertorientierung und Staatsbezug*, Frankfurt/Main, New York, Campus, 1983. Klages, Helmut, *Wertedynamik: über die Wandelbarkeit des Selbstverständlichen*, Zürich/Osnabrück, Fromm, 1988.

Kluckhohn, Clyde, "Values and value-orientations in the theory of action: An exploration in definition and classification", in Talcott Parsons, and Edward Shils (eds.), *Toward a general theory of action*, Harvard University Press, Cambridge, 1951, pp. 383-433.

Kmieciak, Peter, *Wertstrukturen und Wertwandel in der Bundesrepublik Deutschland*, Otto Schwartz, Göttingen, 1976.

Koskela, Hille, *A Two-edged Sword – Public Attitudes Towards Video Surveillance in Helsinki*, The European Group for the Study of Deviance and Social Control, Department of Geography, University of Helsinki, August 2003. http://www.europeangroup.org/conferences/2003/index.htm

Lagazio, M. *Report on research approaches and results,* Deliverable 2.2 of the ETTIS project, 31 June 2012.

"Lawyers.com, 2010 Social Networking Survey Press Release", *Lawyers.com*, 2010. http://press-room.lawyers.com/Lawyerscom-2010-Social-Networking-Survey-Press-Release.html

Livingstone, Sonia, Leslie, Haddon, Anke, Gorzig, and Kjartan, Olafsson, *Risks and Safety on the Internet: The Perspective of European Children: Initial Findings*, London School of Economics, 2010. http://www.ipsos-mori.com/researchpublications/publications/publication.aspx?oItemId=1392

Logica CMG, *e-Identity: European Attitudes Towards Biometrics*, 2006. http://www.eurokiosks.org/whtpapers_logica_e_identity.html

Madden, Mary, Susannah Fox, Aaron Smith and Jessica Vitak, *Pew Internet & American Life Project: Digital Footprints*, Pew Internet & American Life Project, December 2007. http://www.pewinternet.org/Reports/2007/Digital-Footprints.aspx

Madden, Mary, and Aaron Smith, *Pew Internet & American Life Project: Reputation Management and Social Media. How People Monitor Their Identity and Search for Others Online*, Pew Research Center, 26 March 2010. http://pewinternet.org/Reports/2010/Reputation-Management.aspx

Maslow, Abraham, *Motivation and personality*, Harper & Row, New York, 1954.

McKenzie, Betsy, "Out of the Jungle: Digital Footprints Report from Pew", Blog, *Out of the Jungle*, 17 December 2007. http://outofthejungle.blogspot.co.uk/2007/12/digital-footprints-report-from-pew.html

McLaughlin, Barry, "Values in behavioral science", *Journal of Religion and Health*, Vol. 4, 1965, pp. 258-279.

"Most Adults in Largest European Countries, U.S. and China Agree Full Body Scanners Should Be Introduced in Airports", *Reuters*, 3 March 2010. http://www.reuters.com/article/2010/03/03/idUS94073+03-Mar-2010+BW20100303

Musek, Janek, "The universe of human values: A structural and developmental hierarchy", *Studia Psychologica*, Vol. 35, 1993, pp. 321-326.

Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, CA, 2010.

Noyes, Katherine, "Pew Study: Self-Googling on the Rise", *Technewsworld*, 17 December 2007. http://www.technewsworld.com/story/Pew-Study-Self-Googling-on-the-Rise-60810.html

Pauer-Studer, Herlinde, "Privatheit: Ein ambivalenter, aber unverzichtbarer Wert", in Walter Peissl (Ed..): *Privacy. Ein Grundrecht mit Ablaufdatum?*, Wien, Verlag der Österreichischen Akademie der Wissenschaften, 2003, p. 17–30.

Pavone, Vincenzo and SaraDegli Esposto, "Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security", *Public Understanding of Science,* Vol. 21, No. 5, 2010, pp. 556-572.

PEW Internet & American Life Project, "About This Report: Reputation Management and Social Media - Methodology", 26 May 2010. http://pewinternet.org/Reports/2010/Reputation-Management/Methodology/About.aspx

Princeton Survey Research Associates International, *PEW Internet & American Life Project, December 2006 Tracking Survey: Final Topline*, 1 May 2007. http://www.pewinternet.org/Reports/2007/Digital-Footprints.aspx

Ragin, Charles C., *The Comparative Method*, University of California Press, Berkeley, 1987.

Rasmussen, Rune, H., and Sigrun Landro Thomassen, "EU Kids Online: New Approach to Online Safety Required", Kids and Media, 25 October 2011. http://kidsandmedia.org/eu-kids-online-new-approach-to-online-safety-required/

Research Capability Programme Team, *Summary of Responses to the Consultation on the Additional Uses of Patient Data*, NHS: Connecting for Health, 27 November 2009. http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/documents/digitalasset/dh_109343.pdf

Rokeach, Milton, *The Nature of Human Values*, The Free Press, New York, 1973.

Save the Children: Resource Center on Child Protection and Child Rights Governance, "EU Kids Online - Towards a Better Internet for Children", 2012. http://resourcecentre.savethechildren.se/content/library/documents/eu-kids-online-towards-better-internet-children

Schwartz, Shalom H., and Wolfgang Bilsky, "Toward a theory of the universal structure and content of values: Extensions and cross-cultural replication", *Journal of Personality and Social Psychology*, Vol. 58, 1990, pp. 878-891.

Schwartz, Shalom H., "Are There Universal Aspects in the Structure and Contents of Human Values?", *Journal of Social Issues*, Vol. 50, No. 4, 1994, pp. 19-45.

Schwartz, Shalom H., "A Theory of Cultural Value Orientations: Explication and Applications", in Esmer Yilmaz, and Thorleif Pettersson (eds.), *Measuring and Mapping Cultures: 25 Years of Comparative Value Surveys*, Brill, Leiden, 2007, pp. 33-78.

Schwartz, Shalom. H., "A Proposal for Measuring Value Orientations across Nations", Questionnaire Development Report of the European Social Survey, 2003. http://www.europeansocialsurvey.org/index.php?option=com_content&view=article&id=62&Itemid=96

Smith, Peter B., and Shalom H. Schwartz, "Values", in John W. Berry, Segall Marshall H. et al. (eds.), *Handbook of Cross-Cultural Psychology Vol. 3*, Allyn & Bacon, Boston, 1997a, pp. 77-118.

Smith, Peter B., and Shalom H. Schwartz, "Values", in John W. Berry, Marshall H. Segall et al. (eds.), *Handbook of Cross-Cultural Psychology, Vol. 3, Social Behaviour and Applications*, Allyn and Bacon, Needham Heights, 1997b, pp. 77 – 118.

SMSR: Social and Market Strategic Research, *Report on the Findings of the Information Commissioner's Office Annual Track 2010*, Information Commissioners Office, November 2010. http://www.ico.gov.uk/about_us/research/~/media/documents/library/Corporate/Research_and_reports/annual_track_2010_individuals.ashx

Solove, Daniel J., *Understanding Privacy*, Harvard University Press, Cambridge, MA., 2008.

Taylor, Humphrey, *Support for Some Stronger Surveillance and Law Enforcement Measures Continues While Support for Others Declines*, Harris Interactive, 10 September 2002. http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Support-for-Some-Stronger-Surveillance-and-Law-Enf-2002-09.pdf

TNS Opinion and Social, *Special Eurobarometer 335: E-Communications Household Survey*, European Commission, October 2010, p. 157. http://ec.europa.eu/public_opinion/archives/ebs/ebs_335_en.pdf

TNS Opinion and Social, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, Special Eurobarometer, European Commission, 2011. http://ec.europa.eu/public_opinion/archives/eb_special_359_340_en.htm

Turner, Ben, "Americans' Attitudes on Digital Footprints (Pew Internet & American Life Project)", Blog, *Ben Turner's Blog*, 10 September 2009. http://blog.benturner.com/2008/09/10/americans-attitudes-on-digital-footprints-pew-internet-american-life-project/#more-1310

UNISYS Security Index: Global Summary, Lieberman Research Group, 13 April 2012. http://www.unisyssecurityindex.com/usi/global/reports

Vidmar, Neil, and David H. Flaherty, "Concern for Personal Privacy in an Electronic Age", *Journal of Communication*, Vol. 35, No. 2, 1985, pp. 91–103.

Van de Vijver, F. J.R., and Leung, K, "Methods and data analysis of comparative research", in Handbook of cross-cultural psychology, 2nd ed., vol.1, Theory and method, J.W. Berry, Y.H. Poortinga and J. Pandy (eds.), Boston, MA: Allyn & Bacon Inc., 1997b, p.257-300.

Warren, Samuel D.; Brandeis, Louis D., "The Right to Privacy", *Harvard Law Review,* Vol. 4, No. 5, 1890, p. 193–207.

Weber, Max, "Die protestantische Ethik und der Geist des Kapitalismus", in Weber, Max, *Gesammelte Aufsätze zur Religionssoziologie I [1920]*, Mohr, Tübingen, 1988, pp. 17-205.

"Webroot Survey Finds Geolocation Apps Prevalent Amongst Mobile Device Users, But 55% Concerned About Loss of Privacy", *Webroot*, 13 July 2010. http://www.webroot.com/En_US/pr/threat-research/cons/social-networks-mobile-security-071310.html

"Welcome to the URBANEYE Project on CCTV in Europe", URBANEYE, 2004. http://www.URBANEYE.net/index.html

Welzel, Christian, "Werte und Wertewandelforschung", in Viktoria Kaina, and Andrea Römmele (eds.), *Politische Soziologie. Ein Studienhandbuch*, VS Verlag für Sozialwissenschaften, Wiesbaden, 2009, pp. 109-139.

Westin, Alan F., *Privacy and* freedom*,* London, Bodley Head, 1970.

Whitman, James Q., "The Two Western Cultures of Privacy: Dignity Versus Liberty", *Yale Law Journal*, Vol. 113, 2003/04, pp. 1151-1221.

Williams, Robin M., Jr., "Values", in David L Sills (ed.), *International encyclopedia of the social sciences, Vol. 16*, Macmillan, New York, 1968, pp. 283-291.

Yolande E. Chan., Lynda L. Harling Stalker, David Lyon, Andrey Pavlov, Joan Sharpe, Emily Smith, Daniel Trottier and Elia Zurelik*, The Globalization of Personal Data Project: An International Survey on Privacy and Surveillance*, The Surveillance Project, Queen's University, 2008. http://www.sscqueens.org/sites/default/files/2008_Surveillance_Project_International_Survey_Findings_Summary.pdf

Zedner, Lucia, *Security*, Routledge, London, 2009.

Zureik, Elia and L. Lynda Harling Stalker, "The Cross-Cultural Study of Privacy: Problems and Prospects", in Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon and Yolande E. Chan (eds.), *Surveillance, Privacy and the Globalization of Personal Data: International Comparisons*, McGill-Queen's University Press, Montreal & Kingston, 2010.