Surveillance & Society

Article

A gap in the market: The conceptualisation of surveillance, security, privacy and trust in public opinion surveys.

Hayley Watson

Trilateral Research, UK.
hayley.watson@trilateralresearch.com

Rachel L. Finn

Trilateral Research, UK.
rachel.finn@trilateralresearch.com

David Barnard-Wills

Trilateral Research, UK.
david.barnard-wills@trilateralresearch.com

Abstract

Understanding the attitudes of members of the public towards the impact on their privacy of surveillance technologies used to enhance public security is an essential, but complex, consideration for policy makers, where public trust plays a central role. One way of understanding public attitudes is via the assessment of public opinion surveys. However, to ensure that public attitudes are appropriately being measured across all four concepts (privacy, security, trust and surveillance) it is necessary to consider how existing surveys conceptualise and operationalise these terms. This article undertakes precisely this consideration, in order to evaluate existing practices and provide recommendations for future public opinion surveys on surveillance technologies or practices intended to provide security, but which may impact privacy. We have found three issues relating to past approaches: past surveys do not always adequately define or conceptualise the terms they are employing. Second, surveys sometimes rely on the use of examples in lieu of definitions. Finally, and most importantly, we find that existing surveys do not always adequately examine the impact of the public's trust towards the use of surveillance technologies to enhance security, but which may affect their privacy.

Introduction

When discussing national security and/or the protection of citizens, the relationship between privacy and security is often described as a trade-off or a balance (Chandler 2009), particularly in relation to the introduction of new surveillance technologies or practices (Monahan 2006).[1] For example, the European Security Research Advisory Board (ESRAB) (2006) prioritises technology development, particularly surveillance technologies, in its efforts to increase security, which immediately raises questions about privacy and data protection. This has also been reflected in various national policy documents, for example, in a 2009 House of Lords document the author argued that there was a "need to balance national security with human rights" (Quoted in House of Lords Constitution Committee 2009: 64). However, others have argued that the metaphor of a 'trade-off' or 'balance' between privacy and security misrepresents the primary issues, since the erosion of privacy creates new insecurities (Chandler 2009) and privacy is a social good in and of itself (Goold 2009). In some instances privacy may be seen to have eroded in relation to the increasing surveillance of individuals (e.g., communication based surveillance) as highlighted by the 2013 National Security Agency (NSA) scandal, which pointed towards the increase surveillance of civilians in

[1] Please note the clarification of how these terms are understood and employed within this article will take place in the subsequent section.

Watson, H., Rachel L. Finn and David Barnard-Wills. 2017. A gap in the market: The conceptualisation of surveillance, security, privacy and trust in public opinion surveys. *Surveillance & Society* 15(2): 269-285.
http://library.queensu.ca/ojs/index.php/surveillance-and-society/index | ISSN: 1477-7487

the US following the release of confidential documents by Edward Snowden (Greenwald 2014). Furthermore, European policy commitments, such as the Stockholm Programme (2010), argue that in addition to security, privacy and data protection are fundamental rights, which must be adequately protected while ensuring security. Therefore, some elements of the European policy framework seem to be moving away from a balance metaphor (Barnard-Wills 2013). Given this tension within policy documents, this article examines the ways in which previous public opinion surveys conceptualised and operationalised the terms privacy, trust, security and surveillance (i.e., the use of surveillance technologies to enhance security) to determine whether they cohesively and appropriately measure public attitudes in order to adequately inform policy-makers and other stakeholders. The work conducted in this paper, reports findings from part of a wider research project, *PRISMS: The PRIvacy and Security MirrorS 'Towards a European framework for integrated decision making'*, one of the outcomes of which is a Europe-wide survey of citizens' attitudes towards privacy, security, trust and surveillance.

Within PRISMS we aimed to combine these terms to contribute to the creation of a new Europe-wide survey. Prior to doing so, we undertook an examination of how previous surveys have conceptualised and operationalised these terms. As argued by Babbie (2005: 120), within social research adequate conceptualisation is crucial to being able to draw "meaningful conclusions" about the topic that is being investigated, that is clarifying and clearly defining the concepts under investigation. Operationalisation refers to the further defining of variables to enable a concept to be investigated. Within the current study, we chose to examine the conceptualisation and operationalisation of privacy, security, surveillance and trust in past surveys to ensure that, as far as possible, we were able to design a survey that would sufficiently measure European attitudes towards determining whether people evaluate the introduction of security technologies in terms of a trade-off of their privacy. Such a measure was taken to help inform good practices in question design (e.g., avoiding ambiguous questions), and crucially, to enhance the validity and reliability of our results as this is a key priority within survey design. Simply put, reliability refers to the quality of measurement, which would ideally involve collecting the same data if the research was to be conducted with the same sample again (Babbie 2005). Alternatively, validity refers to how accurately the concept is being measured (Babbie 2005). Ensuring the validity and reliability of responses to a survey are essential, particularly when public opinion survey results are utilised to influence policies.

To provide a brief overview of core findings, broadly speaking, in preparing for the survey, our study has revealed that some past surveys do not always adequately define or conceptualise the terms they are employing. For instance of the surveys examined only 11 out of 17 surveys that related to privacy defined what they meant by the term 'privacy'. Furthermore when defining surveillance, 9 out of 12 surveys used examples in lieu of definitions. This is not to say that all surveys use this strategy, but that these findings serve as an important reminder to researchers to take the time to conceptualise their terms and pilot the survey prior to delivery. The absence of clarification of terms may be due to a number of reasons, from the absence of a background document explaining the survey, to a lack of training in survey design on part of the researchers. Still, the consequences can have an impact on the respondents' ability to understand and adequately answer the questions, this in turn, can inhibit the reliability of the results of the survey. Furthermore, by narrowly conceptualising terms, there is also a danger of the validity of the results being affected—which could be avoided in piloting of the survey.[2] This can, consequently, impact officials' understanding of public attitudes towards a phenomenon, such as how people feel about their privacy being invaded to enhance their security, which could serve to inappropriately guide public policies. Secondly, with respect to defining privacy, surveys often use data protection to stand in for privacy when examining public attitudes towards information collection and thus, as outlined above, may neglect other types of privacy worthy of investigation. Finally, when considering the intra-relationship between privacy, security, trust and surveillance, we find that existing surveys do not always adequately examine the impact of the tensions

[2] Please note: this study is based on a secondary analysis of the surveys—further research to liaise with the survey designers may yield interesting insights into why this (at times) narrow conceptualisation may have materialised.

between the different variables and their impact upon one another in the use of surveillance technologies to enhance security. For instance, it is necessary to understand whether the public's trust of surveillance technologies such as CCTV and of those employing those technologies, such as the police, impacts their attitudes towards these surveillance technologies—for mistrust in the police may impact people's perceptions of the value of CCTV cameras for enhancing security As such, it is necessary to examine the impact of these intra-relationships between privacy, trust, surveillance and security to accurately understand public opinion towards the use of surveillance technologies to enhance security.

Surveillance, security, privacy and trust

Surveillance, privacy and security are often interlinked, as authorities procure and deploy surveillance technologies that have significant privacy implications in response to real or perceived security threats. Most famously, the introduction of the government-backed proliferation of CCTV cameras in the UK was interlinked with the James Bulger case (McCahill 2002). Past terrorist events (e.g., the attack on the World Trade Centre in New York, the bombings in Madrid and London) contributed to the implementation of new measures to safeguard from terrorist attacks and opened the door to a variety of measures (e.g., the use of full body scanners in airports) which were potentially intrusive on personal privacy (such as those identified by Bellanova et al. in 2012: visual surveillance, location determination, communication monitoring, biometric identification, dataveillance and sensor technologies). As stated above, in Europe this link between surveillance, security and privacy is exemplified by institutions such as the European Security Research Advisory Board (ESRAB 2006).

Although policy-makers often perceive security as a straightforward concept, within academic circles much attention has been paid to precisely clarifying and outlining what is meant by different types of security (e.g., personal security). Security is applied to a range of different contexts, from social security to technologically secure systems (Lagazio 2012; Nissenbaum 2005). Zedner (2009) 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. Others, such as David Brooks (2009), 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." Being able to define an issue as a security issue is to move it into a different category of political action, to be able to apply different rules and norms, to call upon different actors and institutions, and to orientate oneself towards the issue in a different way (Buzan et al. 1998; Neocleous 2007). Baldwin suggests the necessity of asking security of what: of what values, from what threats, by what means, to what extent, at what cost, and in what time period? Not all of these will be explicit in any given security articulation, and indeed many parts (particular costs) are often not (Baldwin 1997). Much security work in International Relations examines the particular referent object of security (the thing that is to be secured), and 'security' without a referent object makes little sense (Buzan 1991). For Chilton, security is not an isolated concept, but one that is 'implicated in a lexical, semantic and conceptual network in English, having a specific concretisation in the institutionalised discourse of international relations and of the policy-making community itself (Chilton 1996). Chilton does suggest however, that it is most productive to treat the various uses of 'security' as a case of non-arbitrary polysemy rather than as homonyms (words that sound the same, but have fundamentally different meanings) (Chilton 1996). Baldwin argues that 'economic security, environmental security, identity security, social security and military security are different forms of security, not fundamentally different concepts' (Baldwin 1997).

Academics have also found that the concept of privacy is notoriously difficult to pin down. Privacy is widely understood to be a social value and a public good as well as an individual value (Gutwirth 2002; Bennett and Raab 2006; Solove 2008). Although a widely accepted definition of privacy remains elusive, many academics have argued that privacy comprises multiple dimensions. Solove (2008: 9) asserts that privacy is best understood as a 'family of different yet related things'. Roger Clarke outlined, in 1997, a taxonomy of privacy that include four different types of privacy: privacy of the person, privacy of personal data, privacy of personal behaviour and privacy of personal communication. More than a decade later, Finn, Wright and Friedewald (2013) updated Clarke's categories to include seven types of privacy:

1. *Privacy of the person,* which encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private.
2. *Privacy of behaviour and action* concerns activities that happen in public space and private space.
3. *Privacy of personal 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.
4. *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".
5. *Privacy of thoughts and feelings* includes individuals having the right to think whatever they like.
6. *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, and
7. *Privacy of association (including group privacy)* is concerned with people's right to associate with whomever they wish, without being monitored.

However, others have argued that the complexity of privacy as a concept has legal and ethical benefits. The European Court of Human Rights (ECtHR 1992) has ruled that it is neither possible nor necessary to determine the content of privacy in an exhaustive way. 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 (Gutwirth 2002; Sudre et al. 2003).

In the European legal 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. Over the past few years, an intense reform process has led to the recently published Regulation (EU) 2016/679—the General Data Protection Regulation (GDPR). This legislation introduces privacy elements such as supporting 'data protection 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' where there are high risks to rights and freedoms. Developments in the ICT environment (and in particular future and emerging technologies) have created new practices that threaten the privacy of individuals without actually processing their personal data. Indeed, when using various ICTs, individuals leave a vast number of electronic traces (e.g., IP addresses) that are not personal data in the sense of data protection regulations, but which nonetheless become the resources of extensive profiling activities that entail several risks for the privacy of the persons concerned (De Hert and Gutwirth 2008). Therefore, the equation of privacy with data protection does not adequately address infringements that are not directly linked to the processing of personal data.

However, some scholars argue that public 'trust' is implicated in the introduction of surveillance technologies and privacy concepts. Specifically, Lyon (2003) expresses significant concern that post-9/11 security and surveillance measures are characterised by and reinforce a breakdown of trust between individuals and between individuals and the government. Similarly, Nissenbaum (2010) argues that 'spheres of trust' are essential to maintaining privacy as a manifestation of contextual integrity. Furthermore, this sentiment is shared by authorities and policy-makers themselves. A significant sub-set of officials and policy documents describe the need to maintain citizen ‘trust’ in relation to the introduction of surveillance and security technologies that may impact upon privacy. For example, the European Commission’s stated ambition is to implement a security strategy that maintains a high level of citizen trust, by safeguarding individual rights and protecting personal data (European Council 2009; European Commission 2009). Similarly, UK policy documents examining the proliferation of surveillance technologies have argued that a “[l]oss of privacy through excessive surveillance erodes trust between the individual and the Government and can change the nature of the relationship between citizen and state.” (House of Commons 2008: 5). It is for this reason that major surveys on public attitudes towards surveillance, security and privacy often include a consideration of ‘trust’.

In the next section we outline the methodology used to conduct the comparative analysis of previous surveys related to surveillance, security, privacy and trust, before presenting and analysing the results of our examination.

Methodology

PRISMS aimed to analyse 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 examined 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. The project involved a multidisciplinary inquiry into the concepts of privacy and security and their relationships, as well as a EU-wide survey to determine whether people evaluate the introduction of security technologies in terms of a trade-off (Friedewald et al. 2016). As a result, the project aimed to determine the factors that affect public assessment of the security and privacy implications of a given security technology. The project used 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 by taking into account the wider social context (Van Lieshout and Barnard-Wills 2015). In the present paper we present the findings of preparatory research which sought to provide a baseline analysis of existing surveys in order to inform the construction of the PRISMS survey that aims to cohesively examine European attitudes towards this trade-off, and to extract generalisable methodological insights into privacy, security and surveillance survey research.

This study involved compiling a data set of surveys from across the world that focused on exploring public opinion towards surveillance, security, privacy and trust. Researchers began by compiling a data set of approximately 260 surveys, using a review of academic literature, research reports, industry and mass media sources as well as reports by public authorities and industry. The surveys that were collected were conducted by a range of different types of organisations: academic, institutional, funded projects, private market research organisations and government departments. Following the collection, researchers sampled 20 surveys from the larger population of 260 for closer, comparative analysis. Researchers used a deliberative workshop session to select surveys in order to provide a good representation of the following criteria:

- *Topic:* In order to be used in the analysis, the surveys selected for in-depth analysis would have to cover the four issues under examination—surveillance, security, privacy and trust. This would enable researchers to have a clear indication of how each of these issues were conceptualised and operationalised within different surveys.
- *Date range:* from 1997 through to 2011.
- *Sample size:* from smaller samples (less than 1000 participants) to larger representative samples (e.g., as seen with the Eurobarometer studies which sampled up-to 27,000 participants).
- *Sample location:* the surveys included European as well as cross-national samples, including those from: Brazil, Canada, China, Japan, Mexico, New Zealand and the USA). Surveys

were conducted by a range of organisations ranging from academic groups, funded research projects to market research companies (e.g., Queen's University, TNS Opinion & Social and URBANEYE).

- *Language:* English-only for research purposes.

The following table provides further details of the surveys included in the analysis.

Table 1: *Surveys included in the analysis*

Title	***Year***	***Institution***	***Sample***	***Sample size***	***Field(s)***
Information technology and data privacy	*1997*	*INRA (Europe)*	*15 EU Member States*	*16,246*	*Privacy* *Trust*
Support for some stronger surveillance and law enforcement measures continues while support for others declines	*2002*	*Harris Interactive*	*USA*	*2,203*	*Privacy* *Security* *Surveillance*
A two-edged sword—public attitudes towards video surveillance in Helsinki	*2003*	*The City of Helsinki Urban Facts*	*Finland*	*1,240*	*Privacy (indirectly)* *Security* *Surveillance*
CCTV in Europe	*2004*	*Technical University Berlin*	*7 EU countries (Austria, Denmark, Germany, Great Britain, Hungary, Norway and Spain)*	*1,001*	*Privacy* *Security* *Surveillance* *Trust*
e-Identity: European attitudes towards biometrics	*2006*	*LogicaCMG*	*7 EU countries (Czech Republic, France, Germany, the Netherlands, Portugal, Spain, UK)*	*500*	*Security* *Surveillance*
A Survey on EU Citizens' Trust in ID Systems and Authorities	*2007*	*LSE*	*23 EU countries*	*1,906*	*Privacy* *Trust*
Digital Footprints: Online identity management and search in the age of transparency	*2007*	*Princeton Survey Research Associates*	*USA*	*2,373*	*Privacy*
Data Protection in the European Union Citizens' perceptions Analytical Report	*2008*	*Gallup Organization Hungary*	*27 EU Member States*	*27,000*	*Privacy* *Security* *Surveillance* *Trust*
Personlig Integritet: A Comparative Study of Perceptions of Privacy in Public Places in Sweden and the United States	*2008*	*University of Washington, Stockholm University, Seattle Pacific University*	*Sweden and USA*	*600*	*Privacy* *Surveillance*
The Globalization of Personal Data Project: An International Survey on Privacy and Surveillance	*2008*	*Queens University/ Ipsos*	*Cross-national (Canada, USA, France, Spain, Hungary, Mexico,*	*9,606*	*Privacy* *Security* *Surveillance* *Trust*

Title	*Year*	*Institution*	*Sample*	*Sample size*	*Field(s)*
			Brazil, China and Japan)		
Canadians and Privacy	*2009*	*EKOS Research Associates Inc.*	*Canada*	*2,028*	*Privacy* *Security* *Surveillance* *Trust*
Privacy 2.0: personal and consumer protection in the new media reality	*2009*	*SINTEF*	*Norway*	*1,372*	*Privacy*
State of the Nation Survey 2010	*2010*	*ICM*	*UK*	*2,288*	*Privacy* *Security* *Surveillance* *Trust*
Most Adults in Largest European Countries, U.S. and China Agree Full Body Scanners Should be Introduced in Airports	*2010*	*Harris Interactive*	*Cross-national (France, Germany, Great Britain, Spain, USA, Italy and China)*	*7,256*	*Security* *Surveillance*
Unisys Security Index	*2010*	*UNISYS*	*Cross-national (Austria, Belgium, Brazil, Germany, Mexico, the Netherlands, New Zealand, Spain, UK and the US)*	*10,000*	*Privacy* *Security* *Surveillance*
Reputation Management and Social Media. How people monitor their identity and search for others online.	*2010*	*Princeton Survey Research Associates International*	*USA*	*2,253*	*Privacy* *Trust*
Examining the Safety of Children Online Across Europe	*2010*	*Ipsos MORI*	*25 EU countries*	*23,420*	*Privacy* *Security*
Attitudes on Data Protection and Electronic Identity in the European Union	*2011*	*TNS Opinion & Social*	*27 EU Member States*	*26,574*	*Privacy* *Security* *Surveillance* *Trust*
Online Profile & Reputation Perceptions Study	*2011*	*Blueocean market intelligence & Telecommunications Research Group*	*Cross-national (US, Germany, Ireland, Spain and Canada)*	*5,000*	*Privacy* *Security*
Internet Privacy Research	*2012*	*University of Queensland Centre for Critical and Cultural Studies*	*Australia*	*965*	*Privacy*

The sample of surveys assessed for this study were by no means a representative sample of all surveys conducted to understand public attitudes towards surveillance, security, privacy and trust.[3] Rather, the selection was limited to those previously identified in the initial research task, as well as by the deliberation and decision process selected by the researchers. Accordingly, this study involved an exploratory approach to understanding how *some* previous surveys conceptualised surveillance, security, privacy and trust; which is essential for designing and conducting a comprehensive European-wide survey on this matter.

Results

Our study revealed three central findings relating to the conceptualisation of privacy, security, trust and surveillance in existing surveys: vague definitions, a narrow focus in conceptualisation of terms and a missing link in the exploration of the intra-relationship between privacy, security, surveillance and trust.

The first issue relates to the lack of concrete definitions of terms being employed within the survey. Ambiguity could lead to misunderstanding on part of the respondents in providing answers to questions, which could ultimately influence the reliability and validity of the survey. Second, surveys do not always comprehensively conceptualise and subsequently, operationalise the terms under investigation. Specifically, the analysis revealed that at times survey designers utilised a narrow approach to the concept 'privacy' that relied almost entirely on data protection; a similarly narrow approach was sometimes in evidence in relation to the conceptualisation of the term 'security'. When combined with the first finding, unclear conceptualisation and a lack of definition could serve to further affect the validity of a survey and its ability to sufficiently capture public opinion relating to these issues. Lastly, some surveys appear to miss the opportunity to understand the inter-connectedness between surveillance, security, privacy and trust and thus, the PRISMS survey questions could benefit from assessing the impact that one area of consideration has on the other (e.g., the impact of trust of surveillance technologies on the acceptance of surveillance technologies to enhance security).

Vague definitions

Our study revealed that some surveys do not provide concrete definitions of the terms (surveillance, security, privacy and trust) that they are employing in their surveys. Whilst, this may be somewhat difficult to achieve due to individuals perhaps having their own understanding of these concepts, nevertheless it is an important exercise to clarify the ways in which the survey designers are employing the terms. Lack of clarity has the potential to lead to ambiguity and misunderstanding on part of the participant or the researcher's interpretation of the results, which could negatively impact the findings of the surveys, particularly in relation to the validity and reliability of results. Furthermore, some survey designers used examples in lieu of definitions to clarify the terms employed in the question.

The study of existing surveys revealed that the majority of surveys (nine out of 12) that contained questions relating to public perceptions of surveillance directly refer to the term 'surveillance' and develop a wider understanding of what is meant by the term by providing audiences with examples of surveillance technologies, such as cameras, biometrics or body scanners. None of the surveys within the sample provided any direct identification of what the term 'surveillance' meant. Accordingly, confidence is placed in respondents' understanding what these technologies are in order to aid their understanding of the question that they are being asked. When conducting future surveys, it may be necessary for researchers to ensure

[3] It does not, for example, include the most recent surveys conduct in the wake of the Snowdon revelations, such as the Pew Research Centre's *American Attitudes About Privacy and Surveillance* (2015) http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ or *Privacy and Information Sharing* (2016) http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/. However these surveys do appear to have deployed similar methodologies to their predecessors.

that the respondent understands and recognises what these example technologies are. If not, it is essential that the survey provides clarity for the respondent without leading them in any way.

In some instances, surveys associated the term 'surveillance' with terms such as 'recording' and 'monitoring'. For instance, the Eurobarometer referred 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' (TNS Opinion and Social 2011: 64): '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?'

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 security, and thus asks respondents about surveillance in relation to monitoring (The Gallup Organization 2008: 135-136):

> 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?

Thus, our analysis of surveys' findings revealed 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. This was also apparent in questions relating to surveillance employed by the Flash Eurobarometer 225: Citizens perceptions of data protection, where attention is focused on examples of situations where individuals may be monitored, such as through telephone calls, internet usage, credit card use and personal details, when flying to help aid security (The Gallup Organization 2008: 135-136).

In contrast, our review of 17 surveys that assessed public attitudes towards privacy, found that 11 of the surveys directly defined 'privacy'. For instance, *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:

> 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? (INRA 1997: 16)

As seen in the example, the term 'personal tracks' is defined with the use of specific examples to clarify its meaning. Notably, over time, we can see the move towards the use of the term 'personal information', with eight of the 11 surveys defining privacy in this manner. For instance, *Flash Eurobarometer 225: Citizens perceptions of data protection* used the following question to gather individuals' perceptions of the security of their 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?' (The Gallup Organization 2008: 7).

However, there are some surveys that do not define privacy at all. For instance, the *Canadians and Privacy* (2009: Appendix A) survey asked respondents: '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'. Within this survey, new technologies relating to communication included: online social networking sites, cell phones and telecommunications. As illustrated, this question does not provide participants with any indication of what is meant by the term 'privacy' and thus, could lead to issues relating to the validity and reliability of the results (as will be further discussed below). Elsewhere, once again examples are used in lieu of a definition, for instance, the *PEW Internet & American Life Project: Digital Footprints* survey provided the following examples to ask people how important privacy was to them: 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 (Madden and Smith 2007: 2).

Furthermore, our analysis found that those who designed the surveys often did not define the concept '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. This can be observed in the following question, included in the *Flash Eurobarometer 225: Citizens perceptions of data protection*, which asked: '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' (INRA 1997: 24). Elsewhere, some surveys made an effort to use different terms than 'trust' to gain information about public perceptions of the abilities of others to secure their privacy. For instance, the *Globalization of personal data project* use the term 'protection' to point towards the concept of trust in others abilities to protect 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?' (Zureik et al. 2010: 365). The *Special Eurobarometer 359: Data protection and e-Identity* employs a combination of the previous two styles of questioning. The following question 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: '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?' (TNS Opinion and Social 2011: 17)

Elsewhere, there is evidence of the term 'trust' being discussed in an indirect fashion. For instance, the *Eurobarometer 46.1: Information technology and privacy,* 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:

> 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
> 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. (INRA 1997: 24)

Thus, it is evident that while some surveys do not define 'trust', others took measures to indirectly define the term, which with the absence of a definition, goes some way to enabling audiences to understand the meaning of the question they are being asked.

Surveys assessed for this study illustrate that for some surveys, survey designers have chosen not to include a definition of the terms they are employing. Whilst terms such as ‘privacy’ and ‘trust’ may invoke some form of common sense, they are, as established at the beginning of this article, notoriously difficult to define. This could be problematic in that by doing so, researchers may be leaving themselves open to problems relating to the reliability and validity of the results of the survey, particularly if respondents are unsure what the question is asking them. It also creates a situation where different surveys are essentially incommensurate with each other. As Bryman (2008) says, to ensure greater validity of results, researchers should avoid the use of technical terms that respondents may not understand, particularly if they are not going to provide a definition of the term. While not ‘technical’ in the strictest sense, the discussion above demonstrates that terms such as ‘security’ and ‘privacy’ have multiple meanings. In this way, some surveys’ choice of utilising examples may be a useful measure, to be taken into consideration by future survey designers to help gain a more accurate and valid response. Depending upon the survey design, it may not be necessary to deploy a definition in the survey, but a clear conceptualisation is necessary in the *survey design*.

A narrow focus in the conceptualisation of terms

In addition to some surveys being somewhat limited in their defining practices with key concepts, there are also some issues with how surveys are conceptualising and operationalising their terms, particularly in relation to not expanding their understanding of the various components with regard to ‘privacy’ and ‘security’.

As the table below indicates, of the surveys analysed in this study, surveys were most likely to consider five types of privacy (as defined by Finn et al. 2013):

Table 2: Types of privacy discussed in 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*
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 their attention on privacy of data and image. Examples include the following question by the *Flash Eurobarometer 225: Citizens perceptions of data protection*: '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?' (The Gallup Organization 2008: 7). Furthermore, as discussed in the previous section, surveys that focused on other types of privacy often relied upon examples of different surveillance technologies in lieu of a definition 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 measures might have on their civil liberties, however, the term 'civil liberties' was not defined: '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' (Taylor 2002: 3).

Elsewhere, some surveys would assess different types of privacy in a single question. For instance, 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 avoided asking respondents about one particular type of privacy, in this case, privacy of behaviour and action. The survey also asked respondents about their attitudes towards 'privacy of location and space', 'privacy of communication' and 'privacy of data' (TNS Opinion and Social 2001: 64):

> 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.)

Thus, by reviewing surveys relating to privacy, our analysis suggests that there is a gap in current public opinion polls and the way in which they operationalise the term 'privacy', with attention being disproportionately focused on privacy as data protection. As established in the first part of this article, this focus of attention on examining attitudes towards privacy as data protection is also mirrored within a policy context and thus, consequently, may involve the mirroring of attention in public opinion surveys, which seek to inform policy-makers.

As with privacy, as the following table (Table 3) shows, the surveys assessed in the course of this research were commonly focused on three types of security (out of five): physical, radical uncertainty and cyber and information. In addition, one survey assessed economic security.

Table 3: *Types of security discussed in 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*

The concept of security was commonly defined in one of three ways (with the exception of the *Unisys Security Index* which refers to economic 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 question was used within *The Globalization of personal data project* survey: '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?' where respondents are asked about their attitude regarding: community CCTVs (e.g., cameras in public places) and in-store CCTVs (Zureik et al. 2010: 371).

Alternatively, the *State of the Nation* asked people about their view of surveillance technologies, in the form of DeoxyriboNucleic Acid (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 demonstration) should have their DNA records kept on file permanently (The Joseph Rowntree Reform Trust Ltd. and ICM 2010: 6). Here surveillance is used to combat rather than deter crime. 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.

Thus, as with the operationalisation of the concept of privacy, our analysis reveals that the operationalisation of security is somewhat limited within existing surveys. Accordingly, our survey addressed this gap by expanding the way in which questions are asked in relation to these multi-dimensional concepts to ensure we capture the various elements associated with these issues.

A missing link

A central goal of this analysis was to determine how the four terms, privacy, trust, surveillance and security were employed together in existing surveys, and how surveys operationalised and conceptualised these terms. The purpose of this exercise was to inform the construction of a Europe-wide survey whose aim is to understand public attitudes towards the decline in privacy as a result of efforts to enhance security through surveillance technologies. The concept 'trust' is central to this investigation as it plays an important role in influencing public confidence and acceptance of surveillance technologies. Accordingly, a key question was whether and how existing surveys employ these issues as a cohesive whole.

The previous sections of this article reveal that existing surveys commonly discussed security, surveillance and privacy together; however, the issue of trust was not always brought in to the exploration of public opinion towards these inter-related issues. When trust was brought in, it was commonly attributed to discussions surrounding privacy of data and image. For instance, the *Flash Eurobarometer 225: Citizens perceptions of data protection*, asked: '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' (The Gallup Organization 2008: 10). This was similarly seen in other surveys such as *The Globalization of Personal Data project* (2010).

This analysis has therefore shown that 'trust' seems to be commonly treated in isolation, rather than being discussed in relation to the other three concepts, despite its centrality in relation to scholarly and policy discussions around the inter-relationship between surveillance, security and privacy. If, for instance surveys were to ask individuals about their trust of surveillance technologies, rather than limiting their questions to asking about trust of organisations/institutions handling of information, it might help develop a more cohesive understanding of the role that trust plays in shaping public attitudes towards issues surrounding the complex web of privacy, security and surveillance, and therefore how policy makers and other stakeholders might respond to this issue.

Conclusion

This comparative analysis of how existing surveys have conceptualised and operationalised surveillance, security, privacy and trust is an important step in evaluating how valuable these surveys are in adequately informing policy makers, as well as other stakeholders, in public attitudes towards the potential encroachment of privacy to ensure security. As discussed in the methodology section of this paper, the sample of surveys included in this analysis is not a representative sample of existing surveys, and thus, the findings are limited. However, the results do demonstrate several important findings in relation to what contemporary surveys, including the PRISMS survey, should be aware of when designing their surveys.

This analysis of existing surveys has revealed several important findings in relation to how the terms surveillance, security privacy and trust are conceptualised, and thus, the extent to which these surveys are able to capture public attitudes surrounding these matters, particularly in relation to the intra-relationship between these concepts. Specifically, this article has outlined three areas of consideration that are significant and that were put forward for the development of the PRISMS survey.

- First, future surveys ought to address the definition problem. They may try to ensure that they have adequately defined the terms that they employ. Whilst this may be difficult as a result of the lack of clarity over those concepts, which are difficult to narrow down and define in the first place, they should employ the use of carefully crafted examples to help illustrate what is meant by the questions being asked. Such a measure will contribute to enhancing the reliability and validity of the survey. However, fixing definitions is problematic, given that if these definitions do not align with respondent's lived and unconscious versions of the concepts, then the definitions will be poorly operationalised. The challenge comes from assuming a fixed, pre-existing definition. The PRISMS response to this challenge was in many places to avoid the terminology of 'privacy', 'security' etc., but to ask a battery of conceptually related questions, which could then be statistically recomposed into an inductively derived set of 'privacy' and 'security' attitudes (Friedewald et al. 2015).

- Second, the results of this study suggest that future surveys ought to ensure transparency in the rationale behind the design of the surveys and try to ensure that when looking at these inter-related issues, that they adequately conceptualise their concepts under investigation, rather than disproportionately focusing on particular types of surveillance technologies, privacy and/or security. The aim of the PRISMS survey is therefore not primarily to produce topline survey findings (although these produced as a by-product) but rather to build a model of the factors affecting people's acceptance of security and surveillance technologies (Friedewald et al. 2015).
- Finally, it is important that future surveys aim to understand the impact of trust on public attitudes towards the inter-connected relationship concerning public attitudes towards privacy, security and surveillance as this is commonly over-looked.

The process of conceptualising and operationalising key variables in a survey is a challenging task which is compounded by the difficulty in translating those concepts, such as privacy, that are in themselves problematic to define within policy and practice in the first instance. Consequently, it is essential for future surveys to ensure they comprehensively capture public attitudes relating to this complex web of inter-related factors, particularly to support policy-makers, industry professionals and other relevant parties to formulate decisions and recommendations on the ever growing impact of surveillance technologies on the public's right to privacy and security.

Acknowledgements

This paper is based on research performed by the authors as partners in the PRISMS project (Privacy and security mirrors; Grant Agreement No. 285399) funded by the European Commission under its Seventh Framework Programme. The views expressed in this paper are those of the authors alone and are in no way intended to reflect those of the European Commission.

References

Babbie, E. 2005. *The Basics of Social Research,* 4th Edition. Belmont, CA: Thomson Wadsworth.

Baldwin, D. 1997. The Concept of Security. *Review of International Studies* 23: 5-26.

Barnard-Wills, D. 2013. 'Security, privacy and surveillance in European policy documents.' *International Data Privacy Law* 3(3): 170-180.

Bellanova, R., Vermeulen, M., Gurwrith, S., Finn, R., McCarthy, P., Wright, D., Wadhwa, K., Hallinan, D., Friedewald, M., Jeandesboz, J., Bigo, D., Frost, M., and Venier, S. 2012. *Smart Surveillance—State of the Art*, Deliverable 1.1 of SAPIENT project. [Online] Available at: http://www.sapientproject.eu/deliverables.html (accessed 15 February 2013).

Bennett, C. J., and Raab, C.D. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective.* Cambridge, MA: MIT Press.

Brooks, D.J. 2009. 'What is security: Definition through knowledge categorization'. *Security Journal* 23 (3): 225-239.

Bryman, A. 2008. *Social Research Methods*, 3rd ed. Oxford: Oxford University Press.

Buzan, B., Waever, O. and de Wilde, J. 1998. *Security: A New Framework for Analysis*. London: Lynne Rienner.

Buzan, B. 1991. *People, States and Fear:An Agenda for International Security Studies in the Post-Cold War Era* 2nd ed. Boulder, CO: Lynne Rienner.

Chandler, J. 2009. "Privacy versus national security: Clarifying the Trade-off". In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, eds Kerr, I. et al., 121-138. New York: Oxford University Press.

Chilton, P. 1996. *Security Metaphors: Cold War Discourse from Containment to Common House.* New York; Washington; DC; Bern; Frankfurt; Berlin; Vienna; Paris: Peter Lang.

Clarke, R. 1997. 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms', Xamax Consultancy. [Online] Available at: http://www.rogerclarke.com/DV/Intro.html (accessed 15 February 2013).

Council of the European Union. 2010. The Stockholm Programme—An open and secure Europe serving and protecting citizens, 5731/10, Brussels.

De Hert, P., and Gutwirth, S. 2008. 'Regulating Profiling in a Democratic Constitutional State'. In *Profiling the European Citizen: Cross-Disciplinary Perspectives*, eds Hildebrandtand, M., and Gutwirth, S., 271-291. Dordrecht: Springer.

European Court of Human Rights (ECtHR). 1992. *Niemietz vs. Germany* and *Pretty vs. UK,* Judgment of 16 December 1992, § 29. [Online] Available at: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57887 (accessed15 February 2013).

EKOS Research Associated Inc. 2009. *Canadians and Privacy: Final Report*. [Online] Available at: http://www.priv.gc.ca/information/por-rop/2009/ekos_2009_01_e.asp (accessed 15 February 2013).

ESRAB (European Security Research Advisory Board). 2006. '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. [Online] Available at: http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf (accessed 15 February 2013).

European Commission. 2009. "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.

European Council. 2009. The Stockholm Programme—An open and secure Europe serving and protecting the citizens, 17024/09, Brussels.

European Parliament and the Council. 2016. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/446/EC (General Data Protection Regulation), OJ L.119, 4.5.2016.

Finn, R. L., Wright, D. and Friedewald, M. 2013. 'Seven types of privacy'. In *European Data Protection: Coming of Age*, eds Gutwirth, S. Leenes, R., de Hert, P. and Poullet, Y., 3-32. Dordrecht: Springer.

Friedewald, M., van Lieshout, M., Rung, S., Ooms, M., and Ypma, J. 2015. "Privacy and Security Perceptions of European Citizens: A Test of the Trade-off Model". In *Privacy and Identity 2014*, IFIP Advances in Information and Communication Technology 457, eds J. Camenisch et al., 39-53. Cham; Heidelburg; New York; Dordrecht; London: Springer.

Friedewald, M., van Lieshout, M., Rung, S., and Ooms, M., 2016. "The Context-Dependence of Citizen's Attitudes and Preferences Regarding Privacy and Security". In: *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, eds S. Gutwirth, R. Leenes and P. De Hert. Dordrecht: Springer.

Goold, B. 2009. "Surveillance and the Political Value of Privacy". *Amsterdam Law Forum* 1(4): 3-6. [Online] Available at: http://www.amsterdamlawforum.org/ (accessed 5 February 14).

Greenwald, G. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. London: Hamish Hamilton.

Gutwirth, S. 2002. *Privacy and the Information Age.* Lanham, MA: Rowman & Littlefield.

Harris Interactive. 2010. *Most Adults in Largest European Countries, U.S. and China Agree Full Body Scanners Should Be Introduced in Airports*. [Online] Available at: http://www.harrisinteractive.com/vault/HI_FinancialTimes_HarrisPoll_March_2010_02.pdf (accessed 15 February 2013).

House of Commons Home Affairs Select Committee. 2008. *A Surveillance Society?*, Fifth Report of Session 2009-10, HC 58-I. London: The Stationery Office.

House of Lords Constitution Committee. 2009 *Surveillance: Citizens and the State*, Second Report of Session 2008-09, HL Paper 18. London: The Stationery Office.

INRA, Europe. 1997. *Eurobarometer 46.1: Information Technology and Data Privacy*, European Commission. [Online] Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_109_en.pdf (13 February 2013).

Lagazio, M. 2012. "The Evolution of the Concept of Security." *The Thinker* 43: 36-42.

Lyon, D. 2003. *Surveillance after September 11*. Cambridge: Polity Press.

McCahill, M. 2002. *The Surveillance Web: The Rise of Visual Surveillance in an English City*. Devon: Willan.

Madden, M., and Smith, A. 2007. *Pew Internet & American Life Project: Reputation Management and Social Media. How People Monitor Their Identity and Search for Others Online*, Pew Research Center. [Online] Available at: http://pewinternet.org/Reports/2010/Reputation-Management.aspx (accessed 15 February 2013).

Monahan, T., ed. 2006. *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge.

Neocleous, M. 2007. Security, Liberty and the Myth of Balance: Towards a Critique of Security Politics. *Contemporary Political Theory* 6: 131-149.

Nissenbaum, H. 2010. *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Standford, CA: Stanford University Press.

Nissenbaum, H. 2005. "Where Computer Security Meets National Security". *Ethics and Information Technology* 7(2): 61-73.

Solove, D. J. 2008. *Understanding Privacy.* Cambridge, MA: Harvard University Press.

Sudre, F., Marguénaud, J.P., Andriantsimbazovina, J., Gouttenoire, A., and Levinet, M. 2003. *Les grands arrêts la Cour Européenne des Droits de l'Homme.* Paris: Presses Universitaires Française.

Taylor, H. 2002. *Support for Some Stronger Surveillance and Law Enforcement Measures Continues While Support for Others Declines*, Harris Interactive. [Online] Available at: http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Support-for-Some-Stronger-Surveillance-and-Law-Enf-2002-09.pdf (accessed 15 February 2013).

The Gallup Organization. 2008. *Data Protection in the European Union: Citizens' Perceptions - Analytical Report*, Flash Eurobarometer Series #225, European Commission. [Online] Available at: http://ec.europa.eu/public_opinion/archives/flash_arch_239_225_en.htm (accessed 15 February 2013).

The Joseph Rowntree Reform Trust Ltd. and ICM. 2010. *State of the Nation 2010 Poll*. [Online] Available at: http://www.jrrt.org.uk/publications/state-nation-2010-poll (accessed 15 February 2013).

TNS Opinion and Social. 2011. *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, Special Eurobarometer, European Commission. [Online] Available at: http://ec.europa.eu/public_opinion/archives/eb_special_359_340_en.htm (accessed 15 February 2013).

Van Lieshout, M. and Barnard-Wills, D. 2015. *The PRISMS Decision Support System*, PRISMS project deliverable 11.3, 17 July 2015. [Online] Available at: http://prismsproject.eu/wp-content/uploads/2015/07/PRISMS-d11-31.pdf (accessed 19 April 2017).

Zedner, L. 2009. *Security*. London: Routledge.

Zureik, E. and Harling Stalker, L.L. 2010. 'The Cross-Cultural Study of Privacy: Problems and Prospects'. In *Surveillance, Privacy and the Globalization of Personal Data: International Comparisons*, eds Zureik, E., Harling Stalker, L.L., Smith, E., Lyon, D. and Chan, Y.E. Montreal and Kingston: McGill-Queen's University Press.