Innovation: The European Journal of Social Science Research, 2013
Vol. 26, Nos. 1–2, 119–132, http://dx.doi.org/10.1080/13511610.2013.723378

Reconciling privacy and security

Marc van Lieshout[a], Michael Friedewald[b]*, David Wright[c] and Serge Gutwirth[d]

[a]*TNO Information and Communication Technologies, Delft, the Netherlands;* [b]*Fraunhofer Institute for Systems and Innovation Research, Karlsruhe, Germany;* [c]*Trilateral Research & Consulting, London, UK;* [d]*Law Science Technology & Society (LSTS), Vrije Universiteit Brussels, Brussels, Belgium*

(*Received 20 July 2011; final version received 15 August 2012*)

This paper considers the relationship between privacy and security and, in particular, the traditional "trade-off" paradigm. The issue is this: how, in a democracy, can one reconcile the trend towards increasing security (for example, as manifested by increasing surveillance) with the fundamental right of privacy? Our political masters justify their intrusions upon our privacy with proclamations of the need to protect the citizenry against further terrorist attacks like those that have already marred the early twenty-first century. The surveillance industry has been quick to exploit this new market opportunity, supported as it is by inexorable technological "progress" in devising new ways to infringe upon our privacy. The trade-off paradigm has troubled academics. While the European Commission has been devoting billions of euro to security research, it too is troubled by the trade-off paradigm. It is funding the PRISMS project, which will undertake a major public opinion survey on privacy and security and which aims to formulate a decision support system that should offer an alternative to the traditional trade-off model.

Keywords: privacy perceptions; security concern; public opinion; data protection; PRISMS

Introduction

Various governments, and the European Union as a whole, have chosen to invest in new technological devices to foster a proactive attitude against terror (e.g. closed circuit television, passenger scanning, data retention, eavesdropping, biometric passport). Although these technologies are expected to enhance public security, they are subjecting ordinary citizens to an increasing amount of permanent surveillance, potentially causing infringements of privacy and a restriction of fundamental rights.

The relationship between privacy and security has traditionally been seen as a trade-off, whereby any increase in security would inevitably curb the privacy enjoyed by the citizenry. Thus, mainstream literature on the public perception of security technologies generally aims at enquiring how much privacy citizens are willing to trade in exchange for greater security. The trade-off model has, however, been criticized, because it approaches privacy and security in abstract terms, and because it reduces public opinion to one specific attitude, which considers these technologies as useful in terms of security but potentially harmful in terms of privacy.

*Corresponding author. Email: Michael.Friedewald@isi.fraunhofer.de

This paper has two main objectives. First, it considers the right to privacy and the right to security, the relationship between them and the criticism that has been leveled at the traditional trade-off approach. Second, the paper provides the background for a project that aims to devise an alternative to the traditional trade-off model, wherein our political masters, aided and abetted by the security industry, often appear willing to sacrifice some of the citizenry's privacy in order to better secure society against more terrorist attacks such as those that have already marred the early twenty-first century. The paper refers to European policies that support the surveillance and security research funded by the European Commission. In particular, it highlights the PRISMS project, which began in January 2012 and carries on for 42 months. The project aims to conduct a major survey across all EU Member States to gather the views of citizens on privacy and security. It also aims to develop a decision support system for policy-makers and other users of surveillance systems that will help them understand the ramifications of prospective investments in surveillance systems and avoid jeopardizing the European fundamental right to privacy.

The right to privacy

Although the concept of privacy is hard to define precisely, some common understanding of various components of privacy exists. Privacy can be understood as a social value and public good as well as an individual value (Regan 1995; Gutwirth 2002; Bennett and Raab 2006; Solove 2008). Following Solove, Zureik et al. (2010) discern six dimensions of privacy: (1) the right to be let alone; (2) limited access to the self; (3) secrecy; (4) control of personal information; (5) personhood; and (6) intimacy. This is an extension of the distinction made by Alan Westin (1967), differentiating between solitude, intimacy, anonymity and reserve as leading principles indicating the relevance of privacy for individuals. Echoing these multi-dimensional conceptualizations of privacy, the European Court of Human Rights has ruled that it is neither possible nor necessary to determine the content of privacy in an exhaustive way (*Niemietz v. Germany* 1992; *Pretty v. United Kingdom* 2002),[1] and it can thus cover 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; the list is, of course, not exhaustive (Gutwirth 2002; Sudre et al. 2003; Sudre 2005).

However, and in spite of the fact that privacy entails some informational control, not all issues of information control pertain to the privacy of individuals (De Hert and Gutwirth 2009). That is the reason why the European legal framework is composed of both a right to privacy and of a right to the protection of personal data, as embodied by the 2000 EU Charter of Fundamental Rights in its Articles 7 and 8. Therefore, the European regulatory framework is composed of a right centered on the protection of citizens' personal data, and a right protecting the privacy of citizens. Having two separate rights is no coincidence. Indeed, both of them aim at the protection of privacy as a political value, that is, the political private sphere. Yet, they do so by obeying two different constitutional logics, respectively a prohibitive or "opacity" logic, and a regulatory or "transparency" logic. By default, privacy proscribes interferences with one's autonomy, while data protection, by default, acknowledges that the processing of personal data is legitimate if a number of

conditions are met. Privacy shields the citizens and protects their opacity, while data protection accepts the processing of personal data and aims at rendering it transparent (De Hert and Gutwirth 2006). In other words, privacy as a political value is legally embodied in two different rights that both aim at protecting it, although through different means.

The increasing impact of technology on privacy is obvious. Since the first famous incident with privacy intrusion owing to a "mobile camera", eloquently described by Warren and Brandeis (1890), the emergence of ever more intrusive technologies has altered the discourse on privacy fundamentally. People's perception of privacy and the differentiation that can be made between so-called fundamentalist, pragmatic and unconcerned citizens shows change over time but shows some consistency in the distribution among these three groups as well (Kumaraguru and Cranor 2005; similar in Murphy 2007). Surveys indicate that awareness of privacy intrusion is still high while the precise contexts are relevant for the determination of how people experience the intrusions (Attema and de Nood 2010).

In a European policy context, the focus is more on protection of personal data than on the protection of privacy. The first European data protection directive, originating from 1995 (European Parliament and the Council 1995), incorporates principles promulgated in the 1970s and early 1980s (OECD 1980) and that focus on protection of personal data. Judicial and police affairs have been dealt with in separate European directives, and in some sectors (such as health), specific privacy regulations have come into place as well. However, the Data Protection Directive has held the most relevant privacy principles. From May 2009, the Commission undertook an intense round of consultation with stakeholders about the need to update the data protection framework. This eventually led to its publication of a proposal for a Regulation in late January 2012 (De Hert et al. 2012; European Commission 2012). The Commission has proposed a Regulation of the European Parliament and the Council in place of the Directive that it supersedes because the Regulation will be directly applicable in the Member States, unlike the Directive, which had been transposed by the Member States in somewhat different ways. Thus, the Regulation aims to instil much greater harmonization of the data protection framework in Europe and to avoid the fragmentation, the differing rules that have marked the regime until now.[2]

The proposed Regulation, while building firmly on the foundation of the 95/46/EC Directive, introduces many new changes. It enshrines a right to be forgotten (Article 17). The Regulation envisages greater use of privacy by design (data protection by design, Article 23) and the use of privacy seals (Article 39). It has provisions for mandatory notifications of personal data breaches to the data protection authority (Article 31) and data subjects (Article 32). It would make privacy impact assessments (here termed data protection impact assessments) mandatory (Article 33). Companies with 250 employees or more would be obliged to have a data protection officer (Article 35). The Article 29 Working Party would be replaced by a European Data Protection Board (Article 64). Penalties for violating the Regulation would range up to 2% of turnover (Article 79).

Several elements in the draft Regulation make clear that privacy features must be integrated into the entire development process of a system from its earliest conception onwards. Thus, privacy and data protection will be an indistinguishable part of any system and any perceived system change (Hustinx 2010; van Lieshout et al. 2011). The fact that the European Commission is putting an increasing

emphasis upon "privacy-oriented" tools is not a coincidence. Developments in the ICT environment 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 the relevant directives, 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). That is the reason why the amended e-privacy directive (European Parliament and the Council 2002) regulates data that are not *stricto sensu* personal data: traffic and location data. It is, therefore, not without dangers, especially in the field of ICTs, to equate privacy and data protection, since this position fails to deal with infringements upon privacy that are not linked to the processing of personal data.

The right to security

The concept of security is at least as difficult to approach as privacy. Different 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 (Bauman 1999). The German word *Sicherheit* refers to both security and safety while the Dutch and French use two different words as well (*veiligheid* and *zekerheid*, *sécurité* and *sûreté*). Security implies freedom from risks and dangers. It is used in various contexts, from social security to technologically secure systems. Information security is a distinct branch that refers to secure handling of information, preventing unauthorized access and use of data. Secure communications are communications that function as expected and are robust and vital, able to resist attacks on their functionality. For individual citizens, security is related to the absence of dangers with reference to the external environment but also relates to issues of social comfort (family life, health), financial certainties and personal deployment opportunities.

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. This is what the European Commission identifies as belonging to its internal security, and for which it has developed over time a large set of measures and practices (with external security relating to securing the position of Europe vis-à-vis external developments and threats in the external environment). External security relates to maintaining sovereignty in the face of attackers and extends to peace-keeping operations and the like.

With globalization, the rise of new economic superpowers and the accompanying change in power relations, the idea of security in a globalized world is fundamentally more complex and difficult than it used to be. The German sociologist Ulrich Beck points to the detrimental feedback mechanisms that cannot be brought back under control owing to their reflexive characteristics, popping up as unforeseen and unwanted side-effects of previous attempts to control specific societal practices (Beck 1986). The concept present in the work of Beck, Giddens, and Lash (1994) that can serve as a bridge between the concept of privacy and security is the concept of risk. Both privacy and security are related to the notion of risk and risk containment. Containment of risk requires surveillance, directed at natural dangers (e.g. earthquakes) as well as man-made dangers (e.g. nuclear reactors, air traffic). The very

moment surveillance relates to individual persons, however, infringement of privacy may be at stake.

The relationship between privacy and security

Privacy and security are problematic because they are open to a variety of social, political and scientific interpretations and explanations. Each concept needs to be considered in a multidisciplinary way in order to grasp the dynamics that determine the interpretation and evaluation of these concepts by various stakeholder communities. Media, politics, technology, criminology and law all present a different perspective on privacy and security. These perspectives contribute in their own manner to the creation and construction of the public's perception of privacy and security. The challenge is to unravel these various dimensions in the construction of these concepts such that the perspectives and attitudes of citizens can be empirically questioned.

No commonly shared definitions of privacy and security exist. These concepts have contested ontological and epistemological backgrounds, although certain similarities in approach can be discerned. The often heard assumption that privacy is an individual value, reflecting liberal principles about role distribution between citizens and the state, is contested on the ground that this lends too much support for a restrictive policy towards privacy, and that especially the social, collective value of privacy is relevant from a societal and political perspective (e.g. Regan 1995). One can find descriptive accounts of privacy, relating to what privacy *is*, to normative accounts that focus on the *value* of privacy and the level of privacy to be protected. Legal accounts focus on the *right* to privacy and to what extent this should be regulated, while sociological accounts focus on the *interests* that people experience in protecting privacy (for a delimitation of the concepts see Gutwirth et al. 2011).

Can privacy and security be reconciled? There is abundant evidence that many 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. Scarcely a day goes by without stories in the press about how we are losing our privacy as a result of increasingly stringent security requirements.

The traditional "trade-off" model between privacy and security (presupposing citizens make an informed judgement in trading off the one for the other) can be and has been criticized because it is based upon invalid assumptions about people's attitudes and understanding of privacy and security. Both privacy and security are multidimensional and contextual concepts, which cannot be reduced to simplistic descriptions. The systematic recourse to the notion of "balancing" suggests that privacy and security can only be enforced at each other's expense, while the obvious challenge is inventing a way to enforce both without loss on either side.

The often supposed relationship between security and privacy in terms of a trade-off poses an intellectual and policy challenge: is it possible to empirically contest existing ideas that have dominated national and European policy-making for too long, that having more security leads to less privacy?

Reconciling the right to privacy and the right to security

Privacy has often been pitted against other social values, notably security. Policy-makers may curtail privacy for security reasons. After 9/11 and the bombings in

Madrid in March 2004 and London in July 2005, policy-makers in the United States, the UK, the EU and elsewhere took a number of initiatives, supposedly in the interests of making our society safer against the threats of terrorism. For example, the Bush administration in the United States engaged in warrantless telephone intercepts. The EU introduced the Data Retention Directive whereby electronic communications suppliers were required to retain certain phone call and e-mail information, although not the actual content, for up to two years. Many critics regarded such measures as an infringement of privacy. Our privacy was being traded off against security (or security theater, to use Bruce Schneier's term), the effectiveness of which has been called into question.

It is not just our political leaders who engage in the process of balancing privacy against other values, in this case security. Virtually all stakeholders are engaged in this balancing process, often on a daily basis. Individuals make trade-offs when they consider how much personal data they are willing to give to service providers in exchange for a service. Industry players, concerned about trust and reputation, must balance their desire to collect as much personal data of their customers as possible against the potential reaction of their customers to undue intrusion. The same media who rail against the laxity of governments and companies in not preventing data theft or loss are often engaged in reporting on the "private" lives of public figures, sometimes illegally by intercepting mobile calls (Marsden 2009). Governmental officials share personal data in an effort to counter benefit fraud or to detect children at risk of abuse.

Much has been written in academic journals (and elsewhere) about the trade-offs between privacy and other social values, notably security. Many scholars see the trade-off as problematic because it weighs apples and oranges: how can one weigh one value (privacy) against another value (security), which are two different values? If privacy is regarded as a cornerstone of democracy,[3] then sacrificing privacy in the name of security undermines democracy itself. Do we want to be completely secure in a police state? Lucia Zedner (2009, 135–136) concisely points out the problems with the balancing metaphor.

> First . . . rebalancing presupposes an existing imbalance that can be calibrated with sufficient precision for it to be possible to say what adjustment is necessary in order to restore security. Yet terrorist attacks create a political climate of fear that is not conducive to sober assessment of the gravity of the threat posed . . .
>
> A second ground for caution is the question of whose interests lie in the scales when rebalancing is proposed. This issue is generally fudged by the implicit suggestion that security is to be enjoyed by all. In practice the balance is commonly set as between the security interests of the majority and the civil liberties of that small minority of suspects who find themselves subject to state investigation . . . The purported balance between liberty and security is thus in reality a "proposal to trade off the liberties of a few against the security of the majority" . . .
>
> Third, claims to rebalance rarely entail a close consideration of what lies in the scales. Any talk of balancing implies commensurability, but . . . there are at least two grounds for doubting the commensurability of security and liberty interests. The first is that, as we have already observed, we are weighing collective interests against those of small minorities or individuals. The second is what might be called temporal dissonance, namely the fact that we seek to weigh known present interests (in liberty) against future uncertainties (in respect of security risks). Although the certain loss of liberty might be expected to prevail over uncertain future security benefits, future risks tend to outweigh present interests precisely because they are unknowable but potentially catastrophic. Fundamental rights that ought to be considered non-derogable and to be protected are placed in peril by the consequentialist claims of security.

> Together, these concerns should provide a powerful check upon demands to rebalance in the name of security. As Thomas concludes: "the idea of trading off freedom for safety on a sliding scale is a scientific chimera . . . Balance should not enter the equation: it is false and misleading" . . . Given the powerful political appeal of balancing, the primary challenge is to find an alternative rhetoric with which to frame the debate.

Finding a credible, alternative rhetoric remains a challenge. This perhaps accounts for the somewhat schizophrenic policies that have characterized the approaches adopted by governments and the EU. Policy-makers wish to be seen adopting a tough approach against terrorism – to protect democracy – yet at the same time at least some of them recognize that the measures adopted threaten the very democratic values and fundamental rights, including perhaps especially privacy, they seek to protect. In the next section, we review and discuss the key policies that have framed this debate at the European level.

EU security policies

The European Commission's security strategy has evolved from various programs and actions. Over the past decade, the Tampere program (1999–2004), the Hague program (2005–2009) and most recently the Stockholm program (2010–2014) form the basis of the Commission's internal security strategy. Various events (the attack on the World Trade Center 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 that were potentially intrusive on personal privacy (such as CCTV and biometric identification techniques).

The new security threats and challenges after the 9/11 attacks were recognized in December 2003 with the adoption of the EU Security Strategy (Council of the European Union 2003) and the European Commission's decision to establish an EU Security Research Programme (ESRP). As a first step, the European Commission decided to form a "Group of Personalities" (GoP) with members from the Commission, research institutions and the European security and defense industry to oversee the development of the ESRP. In their report, presented in March 2004, the GoP stated that the EU needed to develop capabilities to protect the security of its citizens and that "Europe must take advantage of its technological strengths" to achieve these goals (Group of Personalities in the field of Security Research 2004). The European Commission seized upon these suggestions in its Communication on security research (European Commission 2004b) and the subsequent enhancement of European industrial potential in the field of security research (European Commission 2004a). It specified in its 2006 Security Research Agenda that security research should be aimed at identifying and protecting against unlawful or intentional malicious acts harming European societies (European Security Research Advisory Board 2006). The GoP report makes the point that "technology itself cannot guarantee security, but security without the support of technology is impossible". It provides public authorities with information about threats, which is needed to build effective protection against them.

The European Security Research Advisory Board (ESRAB), which was established to provide advice to the European Commission and to oversee the ESRP, explained in 2006 that

> improving situation awareness and assessment [requires] the capture, fusion, correlation and interpretation of disparate forms of real-time and historical data and their presentation in a clear manner, facilitating effective decision-making and performance in a complex environment. Interoperable databases will be essential to allow surveillance information to be cross-referenced against multiple heterogeneous sources. (European Security Research Advisory Board 2006)

This statement basically says 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. Many of the projects funded under the European Commission's Preparatory Action for Security Research and in the first two calls on security research in the EC's Seventh Framework Programme concern this kind of surveillance technology. The necessity of (smart) surveillance is especially stressed for border security, protection against terrorism and organized crime, and critical infrastructure protection (European Security Research Advisory Board 2006).

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 behavior and fighting illegal immigration (European Commission 2010b). It identifies 18 different initiatives, some of which were established several years ago (e.g. the Schengen Information System) and others are the result of the heightened threat alerts in recent years. Some are still in the stage of implementation, such as the Registered Travellers Programme (part of the Smart Borders Package) for which legislation is expected in 2012 (European Commission 2011).

In its analysis, the Commission concludes that most systems are functionally separate and have separate legislation covering their operation, thus building in safeguards for function creep, that is, the danger arises when a system can be used for other functions or purposes in addition to those originally envisaged, thereby potentially eroding data protection safeguards. On the other hand, the Commission acknowledges that many systems collect similar data (15 out of 18 collect biometric data) that could be shared to validate, update or complete data sets. Six out of 18 initiatives are centralized systems, and many use the same secured European infrastructure (European Commission 2006). In addition the Commission proposes a centralized IT agency to help improve operating centralized and decentralized data exchange practices.

Regulations concerning data retention vary considerably, from 24 hours for Advanced Passenger Information to 15 years for Passenger Name Records collected by the United States. Although a formal review process for all initiatives is in place, hard evidence for the effectiveness of the initiatives is lacking. For some initiatives, anecdotal evidence is presented that shows beneficial effects of some measures (the Data Retention Directive, Cybercrime Alert Platforms, Europol, Eurojust, Passenger Name Records, Terrorist Finance Tracking Programme) and for other initiatives, figures are presented on assets or items collected, but no systematic appraisal of the effectiveness of surveillance systems is presented. No information is provided about the acceptance of these systems by European citizens nor the extent to which they trust surveillance initiatives for improving their security.

Recognizing this problematic potential of surveillance technologies, the Commission stated as early as 2004 that in security research "individual rights, democratic values, ethics and liberties need to be respected. A balance must be struck between surveillance and control to minimize the potential impact of terrorist action, and

respect for human rights, privacy, social and community cohesion and the successful integration of minority communities'' (European Commission 2004b). The EC's 2009 Communication on freedom, security and justice reinforced this claim: ''The area of freedom, security and justice must above all be a single area in which fundamental rights are protected, and in which respect for the human person and human dignity, and for the other rights enshrined in the Charter of Fundamental Rights, is a core value'' (European Commission 2009). The same Communication goes on to state that the EU must be increasingly aware of privacy and data protection issues related to emerging technologies and act accordingly in order to fulfil the above claim.

The Commission seems intent on implementing its security strategy while maintaining a high level of trust by citizens in its activities, by safeguarding individual rights and protecting personal data. As indicated above, the various Communications published in recent years reflect this ambition, although the undertone of the GoP and ESRAB reports and the nature of the technologies funded by the Commissions (European Commission, DG Enterpise and Industry 2009) raise doubts that equal weight is given to privacy and security.

The PRISMS project: a survey on privacy and security

The Commission has questioned the privacy–security trade-off paradigm. In 2010, in a call for proposals in the Security research program under its Seventh Framework Programme, the Commission has posed questions such as:

- Do people actually evaluate the introduction of new security technologies in terms of a trade-off between privacy and security?
- What are the main factors that affect public assessment of the security and privacy implications of given security technology?

Addressing these questions is not simply a matter of gathering data from a public opinion survey, as such questions have intricate conceptual, methodological and empirical dimensions. Citizens are influenced by a multitude of factors. Privacy and security may be experienced differently in different political and socio-cultural contexts. No more than two decades ago Europe was characterized by a political landscape in which different political systems co-existed. This has affected how people perceive concepts such as trust, accountability, concern and the like in relation to the state (Castles 1993), rendering a uniform empirical approach to researching these concepts into a difficult challenge. Socio-cultural differences throughout Europe are such that no uniform empirical approach to researching how people perceive concepts such as privacy, trust, security and concern can be adopted. Until now, no survey or study has yet addressed the facets in a comprehensive way across all Member States.[4]

The Commission also called for development of a decision support system to be provided to users of surveillance systems to help give them insight into the pros and cons of specific security investments compared with a set of alternatives taking into account a wider societal context.

A consortium[5] responded successfully to this call and, accordingly, the Commission is funding the PRISMS (Privacy and Security Mirrors: Towards a European framework for integrated decision making) project, which intends to

critically examine the validity of the trade-off concept and to propose an alternative paradigm (e.g. privacy risk management) in order to arrive at a more sophisticated approach to the relationship between privacy and security. The consortium will address the above questions and related questions by means, *inter alia*, of a survey of the European population. The project was launched in February 2012 and goes on for 42 months.

The PRISMS project starts with a multidimensional analysis of the relation between privacy and security from the different perspectives of technology, policy, media, criminology and law. These diverse perspectives offer the analytical background against which perceptions and attitudes of citizens can be studied. The consortium is also determining the factors that affect public assessment of the security and privacy implications of a given security technology. Having analyzed the conceptualizations of and interrelations between privacy and security, the consortium plans to test and validate its analysis in interviews, focus groups and workshops that will bring together various stakeholder groups (citizens, policy advisors, security people, societal organizations, criminologists and techno-political scientists).

The core of PRISMS will be a full-fledged survey that investigates the opinions, attitudes and behavior of a representative sample of 1000 citizens from each of the 27 Member States of the Union on privacy and security. The project will use these results in devising a decision support system providing users (those who deploy and operate security systems) with insight into the pros and cons, constraints and limits of specific security investments compared with alternatives taking into account a wider societal context. The decision support system will need to reconcile the various dimensions such that the results can be understood in terms of discriminating between options for security investments.

There seems to be only one precedent for a cross-national study of citizens' attitudes towards security and privacy, that is, a project organized and led by the Queen's University in Canada (Zureik et al. 2010), which conducted a survey in eight countries. That study noted a clear and striking absence of surveys on attitudes towards privacy and security. It concluded that analyzing attitudes is relevant, given current developments that confront citizens with transborder data flows in everyday situations (e.g. banking, traveling), but it warned against a too simplistic approach of surveying these attitudes. Methodological problems abound and need to be taken into account. Differences may arise in responses owing to the sequence of questions. Having a question on a security incident before a question on privacy may lead to different outcomes than posing the questions the other way around. In addition to these methodological problems, researchers face substantive problems with understanding the concepts of privacy and security. The survey performed by the Queen's University took several years from initiation to completion, and only recently has been finalized in a book providing the main results. The PRISMS consortium will use the expertise built up during the eight-country survey by Queen's University. Indeed, two researchers from that study are also partners in the PRISMS project as well as an affiliate of the organization that conducted the survey.

The PRISMS approach is characterized by a strong emphasis on practical cases, to be used as hypotheses and testing grounds in the survey to be undertaken by the consortium. This is prerequisite to get results that are easily understood and that can be interpreted over various demographic, geo-spatial and socio-cultural clusters existing within Europe. The survey and multidimensional analysis will provide input

necessary for the creation of the decision support system. The various analyses will help in the construction of hypotheses that will be tested in the survey, but they also have a value in their own respect. In this manner, the various approaches (technological, policy, criminological, media, legal) will add value to the body of knowledge of the disciplines to which they belong while offering cross-disciplinary results as well.

Throughout the entire project, there will be extensive stakeholder interaction and consultation in various forms. Stakeholders vary from institutional actors and policy-makers to the public at large. In the early phases of the project, interaction with stakeholders will be dedicated to obtaining a better understanding of their perceptions and attitudes vis-à-vis the key concepts and approaches of our project. In the later phases of the project, interaction is dedicated more to arriving at a shared understanding of how stakeholders can profit from the results of the project and what constraints the decision support system might encounter. Throughout the entire project, the consortium will use resources to inform stakeholders and the broader community on the existence of the PRISMS project, the intermediate results and the manner in which one could become more engaged with the project.

The decision support system will support stakeholders in making a decision about security investments to be made. A decision support system might have the connotation of a push-button system that yields specific outcomes based on specific inputs. The consortium considers such a decision support system not to have much practical value given the complexity of the situations for which security investments have to be made. The system is meant to support the decision-making process, and not to be a system that makes the decisions itself. The decision support system will combine substantive principles with process-oriented principles, offering state-of-the-art insights in how to arrive at the most optimal approach and solution. It will help in understanding the consequences of specific decisions and in incorporating insights on perspectives and attitudes of citizens in realizing the best of possible systems needed to assure a secure Europe while maintaining the highest level of privacy and data protection.

Acknowledgment

Among other sources, this paper draws on research carried out in the EC-funded FP7 project PRISMS: The Privacy and Security Mirrors: Towards a European framework for integrated decision making (FP7-SEC-2010-285399).

Notes

1. § 29 of the Niemietz judgment says: "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."
2. In its regulatory reform package officially released on 25 January 2012, the Commission also proposed a Directive "on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data".

3. The Supreme Court of Canada has stated that "society has come to realize that privacy is at the heart of liberty in a modern state … Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual" (*R. v. Dyment* 1988). Goold (2009) states: "Without privacy, it is much harder for dissent to flourish or for democracy to remain healthy and robust. Equally, without privacy the individual is always at the mercy of the state, forced to explain why the government should not know something rather than being in the position to demand why questions are being asked in the first place."
4. The European Commission's (2010a) Internal Security Strategy action plan, released in late November 2010, and its Communication on the Stockholm Programme (European Commission 2009), released in June 2009, are strong indicators of the increasing policy importance attached to security and privacy and of the need to take both into account in decision-making.
5. The PRISMS consortium comprises eight partners: Fraunhofer Institute for Systems and Innovation Research, Karlsruhe, Germany (co-ordinator); Trilateral Research & Consulting LLP, London, UK; Vrije Universiteit Brussels, Research Group on Law Science Technology and Society, Belgium; TNO Information and Communication Technologies, Delft, The Netherlands; the University of Edinburgh, UK; Eötvös Károly Institute, Budapest, Hungary; Zuyd University, Infonomics and New Media Center, Maastricht, The Netherlands; and Ipsos MORI, London, UK.

References

Attema, J., and D. de Nood. 2010. *Over de rolverdeling tussen overheid en burger bij het beschermen van identiteit* [About the roles of government and citizens in the protecting indentity]. Leidschendam: ECP-EPN.

Bauman, Z. 1999. *In Search of Politics*. Cambridge: Polity Press.

Beck, U. 1986. *Risikogesellschaft: Auf dem Weg in eine andere Moderne* [Risk society – towards a new modernity]. Frankfurt am Main: Suhrkamp.

Beck, U., A. Giddens, and S. Lash. 1994. *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order*. Stanford, CA: Stanford University Press.

Bennett, C. J., and C. D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. 2nd ed. Cambridge, MA: MIT Press.

Castles, F. G. 1993. *Families of Nations: Patterns of Public Policy in Western Democracies*. Aldershot: Dartmouth.

Council of the European Union. 2003. "A secure Europe in a better world – the European Security Strategy." Approved by the European Council held in Brussels on 12 December 2003 and drafted under the responsibilities of the EU High Representative Javier Solana, Brussels.

De Hert, P., and S. Gutwirth. 2006. "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power." In *Privacy and the Criminal Law*, edited by E. Claes, A. Duff, and S. Gutwirth, 61–104. Antwerp: Intersentia.

De Hert, P., and S. Gutwirth. 2008. "Regulating Profiling in a Democratic Constitutional State." In *Profiling the European Citizen: Cross-disciplinary Perspectives*, edited by M. Hildebrandt and S. Gutwirth, 271–291. Dordrecht: Springer.

De Hert, P., and S. Gutwirth. 2009. "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action." In *Reinventing Data Protection?*, edited by S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, and S. Nouwt, 3–44. Dordrecht: Springer.

De Hert, P., V. Papakonstantinou, D. Wright, and S. Gutwirth. 2012. "Principles and the Proposed New Data Protection Regulation." *Innovation: the European Journal of Social Science Research*, 25 (this issue).

European Commission. 2004a. *On the Implementation of the Preparatory Action on the Enhancement of the European Industrial Potential in the Field of Security Research, Towards a Programme to Advance European Security Through Research and Technology*. COM(2004) 72 final. Brussels European Commission.

European Commission. 2004b. *Security Research: the next steps*. COM(2004) 590 final. Brussels European Commission.

European Commission. 2006. "European Commission Signs 210 Million New Contract to Create Safer EU IT Network." Press release IP/06/1301.

European Commission. 2009. *An Area of Freedom, Security and Justice Serving the Citizen*. COM(2009) 262 final. Brussels: European Commission.

European Commission. 2010a. *The EU Internal Security Strategy in Action: Five Steps Towards a more Secure Europe*. COM(2010) 673 final. Brussels: European Commission.

European Commission. 2010b. *Overview of Information Management in the Area of Freedom, Security and Justice*. COM(2010) 385 final. Brussels: European Commission.

European Commission. 2011. *Smart Borders – Options and the Way Ahead*. COM(2011) 680 final. Brussels: European Commission.

European Commission. 2012. *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: European Commission.

European Commission, DG Enterpise and Industry. 2009. *Towards a more Secure Society and Increased Industrial Competitiveness: Security Research Projects Under the 7th Framework Programme for Research*. Brussels: European Commission.

European Parliament and the Council. 1995. "Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data on the Free Movement of Such Data." *Offficial Journal* L281: 31–50, November 23.

European Parliament and the Council. 2002. "Directive 2002/58 of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector." *Offficial Journal* L201, 37–47, July 31.

European Security Research Advisory Board. 2006. *Meeting the Challenge: The European Security Research Agenda. A Report from the European Security Research Advisory Board*. Luxembourg: Office for Official Publications of the European Communities.

Goold, B. J. 2009. "Surveillance and the Political Value of Privacy." *Amsterdam Law Forum* 1 (4): 3–6.

Group of Personalities in the Field of Security Research. 2004. *Research for a Secure Europe*. Luxembourg: Office for Official Publications of the European Communities.

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

Gutwirth, S., R. Gellert, R. Bellanova, M. Friedewald, P. Schütz, D. Wright, E. Mordini, and S. Venier. 2011. *Legal, Social, Economic and Ethical Conceptualisations of Privacy and Data Protection. Deliverable 1, The Prescient Project* [Online]. Accessed December 12. http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf

Hustinx, P. 2010. "Privacy by Design: Delivering the Promises." *Identity in the Information Society* 3, 253–255.

Kumaraguru, P., and L. C. Cranor. 2005. *Privacy Indexes: A Survey of Westin's Studies*. CMU-ISRI-05-138. Pittsburgh, PA: Carnegie Mellon University [Online]. Accessed December 12, 2011. http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf

Marsden, S. 2009. "Phone 'blagging' methods exposed." *The Independent*, 9 July [Online]. Accessed December 12, 2011. http://www.independent.co.uk/news/uk/crime/phone-blagging-methods-exposed-1739387.html

Murphy, O. 2007. *A Surveillance Society: Qualitative Research Report*. Wilmslow: ICO.

Niemietz v. Germany. 1992. 72/1991/324/396, December 16. Council of Europe: European Court of Human Rights [online]. Accessed December 12, 2011. http://www.unhcr.org/refworld/docid/3f32560b4.html

OECD. 1980. *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*. Paris: Organisation for Economic Co-operation and Development.

Pretty v. United Kingdom. 2002. Application no. 2346/02, 29 April. Council of Europe: European Court of Human Rights [online]. Accessed December 12, 2011. http://www.unhcr.org/refworld/docid/4daee1682.html

R. v. Dyment. 1988. CanLII 10 (SCC), [1988] 2 SCR 417 [online]. Accessed December 12, 2011. http://canlii.ca/t/1ftc6

Regan, P. M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill, NC: University of North Carolina Press.

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

Sudre, F. 2005. "Rapport introductif: La construction par le juge européen du droit au respect de la vie privée" [The right privacy under the European Convention on Human Rights]. In *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme* [Introductory report: The construction of the right to privacy by the European Courts], edited by F. Sudre. Brussels: Bruylant.

Sudre, F., J.-P. Marguénaud, J. Andriantsimbazovina, A. Gouttenoire, and M. Levinet. 2003. *Les grands arrêts de la Cour Européenne des Droits de l'Homme* [The major judgements of the European Court of Human Rights]. Paris: Presses Universitaires Française.

van Lieshout, M., L. Kool, B. van Schoonhoven, and M. de Jong. 2011. "Privacy by Design: An Alternative to Existing Practice in Safeguarding Privacy." *Info* 13 (6): 55–68.

Warren, S. D., and L. D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4 (5): 193–220.

Westin, A. F. 1967. *Privacy and Freedom*. New York: Atheneum.

Zedner, L. 2009. *Security. Key Ideas in Criminology*. London: Routledge.

Zureik, E., L. H. Stalker, E. Smith, D. Lyon, and Y. E. Chan. 2010. *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*. Montreal: McGill–Queen's University Press.