The PRIvacy and Security MirrorS: “Towards a European framework for integrated decision making”

Final Report Summary - PRISMS (The PRIvacy and Security MirrorS: “Towards a European framework for integrated decision making”)

Executive Summary:
The EU FP7 Security Research project PRISMS was launched to investigate the relationship between security and privacy perceptions of European citizens. This relation is commonly positioned as a ‘trade-off’, and accordingly infringements of privacy are sometimes seen as acceptable or even required costs of enhanced security.
This common understanding of the security-privacy relationship has informed and influenced security policies and measures across the EU. However, an emergent body of scientific work and public scepticism question the validity of the security-privacy trade-off. In response to these developments, PRISMS has researched the relation between surveillance, privacy and security from a scientific as well as citizen’s perspective. A major aim of was to contribute with its results to the shaping of security technologies and measures as effective, non-privacy-infringing and socially legitimate security devices in line with human rights and European values.

PRISMS contributed to this objective in different ways. Main results of the research conducted are:

- The comparison of the most important security challenges, as perceived by citizens and by experts, with security policies on the European and national level shows a considerable mismatch; where’s concerns are mainly of economic and social nature, policies are focused on fighting crime and terrorism by surveillance technologies.

- The analysis of important security technologies and practices from different disciplinary showed that in most cases technology development is dominated by security thinking while privacy aspects are usually neglected (or passed on to other actors).

- The pan-European survey involving 27,000 citizens in 27 EU member states provided a comprehensive picture of citizen’s knowledge about privacy and security topics, their general perception of security and privacy and an assessment of several specific security practices.

- The development and testing of a model of criteria and factors influencing acceptability of surveillance based security technologies showed that the trade-off approach is by far oversimplifying the existing complex relationships. This approach is therefore not suitable to inform policy-making.

- The development and testing of a of a decision support system (DSS) for the involvement of citizens in future security related decision-making based on the theoretical considerations and empirical finding. The tool was successfully tested in two different test cases, providing in-depth information on practical aspects of participatory assessment.

- The organisation of a two days joint international conference organised by PRISMS together with the SurPRISE, and PACT projects was the highlight of the dissemination activities.

Project Context and Objectives:
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 criticised, 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.

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, though 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 which 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 criticised because it is based upon invalid assumptions about people’s attitudes and understanding of privacy and security. Both privacy and security are multi-dimensional 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 which have dominated national and European policy-making for too long, that having more security leads to less privacy?

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 US, the UK, 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 US 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, though 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 theatre, 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, 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, 135-6) 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 characterised 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 recognise that the measures adopted threaten the very democratic values and fundamental rights, including perhaps especially privacy, they seek to protect.

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.

Like many scholar the European Commission has questioned the privacy-security trade-off paradigm in a call for proposals in 2010 that would address 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 in the PRISMS project 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 characterised 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 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.

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 to a set of alternatives taking into account a wider societal context.

The PRISMS approach is characterised 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 provide input necessary for the creation of the decision support system. The various analyses helped in the construction of hypotheses that were 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) added 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 was an extensive stakeholder interaction and consultation in various forms. Stakeholders vary from institutional actors, policy makers to the public at large. In the early phases of the project, interaction with stakeholders was dedicated to get 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 how stakeholders can profit from the results of the project and what constraints the decision support system should meet.

The decision support system was designed to supports stakeholders in deciding 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. We consider 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 combines substantive principles with process-oriented principles: offering state-of-the-art insights in how to arrive at the most optimal approach and solution. It helps in understanding the consequences of specific decisions and in incorporating insights on perspectives and attitudes of citizens in realising the best of possible systems needed to assure a secure Europe while maintaining the highest level of privacy and data protection.

References


Project Results:

Socio-technical analysis

The PRISMS project analyses the traditional trade-off model between privacy and security and devises a more evidence-based perspective for reconciling privacy and security, trust and concern. A number of activities have been employed in the project, including an analysis of security and privacy technologies (of
which this deliverable is part), a policy assessment, a criminological analysis, a legal perspective, a discourse analysis of media attention to privacy, security and trust issues, an analysis of existing public opinion surveys, and a survey of citizens’ privacy and security perceptions.

A first part was the analysis of technological trends in privacy and security technologies. The analysis was done from two perspectives: one in which we present the findings of an analysis of the current trends as these can be derived from technology roadmaps, technology policy documents and information on European research projects in the security field; and one in which we adopt a sociological perspective in which we analyse six cases of security and privacy technologies using the conceptual background of Science and Technology Studies (mutual shaping of technology and society).

Together, the two perspectives break open the black box of security and privacy technologies. They show that security is still the most relevant driver of current developments. Privacy technologies do not have the same standing as security technologies. Not at all, we could add. While security technologies are framed through security roadmaps, outlining which building blocks and security systems need to be in place in order to arrive at the desired ‘systems of systems’ that should help safeguarding society from a variety of threats, no such roadmap exists for privacy technology. Privacy technologies lack the institutional backing that is so visible for the security domain. On the other hand, we did signal a growing awareness for the potential of privacy technologies, also in the context of security threats. This goes hand in hand with the growing interest and attention for Information and Communication Technologies (ICT), cybersecurity and critical infrastructures (ICT-networks). ICTs are generally seen as the enabling technologies (building blocks) for a large variety of security technologies. The framing of threats to society such that it inevitably leads to the need for investments in security technologies can be seen in the organisation of the various security work programmes of the European Commission. In these work programmes, every now and then one can notice attention for broader perspectives on security issues (one of which led to the realisation of PRISMS, and together with PRISMS of PACT and SurPRISE).

The second part dealt with six cases that together shed light on how discourses on privacy and security technologies are framed and how this framing leads to apparently inevitable design choices. These design choices usually promote security above privacy considerations. The cases show how in specific circumstances privacy considerations sometimes frame specific user groups. The case of the body scanners for instance shows how a specific group of users (patients with a stoma) face considerable problems due to the framing of the body scanners of deviate bodily objects. The case of smart grids sheds light on the redefinition of the concept of informational self-determination, due to the potentially excessive collection of personal data. Since smart meters are placed in households, the privacy of individual persons becomes merged with the privacy of the household, usually encompassing a few or sometimes even several persons. The case of biometrics shows how identities are constructed through use of biometric access control technologies. Through deep packet inspection it becomes possible to analyse the digital content of packages which are sent over the Internet. While this is usually not the intention (deep packet inspection essentially refers to the ability to ‘read’ the headers of the packages and not the content itself), the discourse on DPI shows how people consider their privacy to be infringed and how they fear the big brother perspective that comes with DPI. In that sense, it is interesting to note how a by itself technical analysis can turn into a social issue. This indicates the intrinsic moral properties that technological devices may have, and which may go far beyond the imagination of the designers of these technologies. Finally,
the case study on drones show how accountability and responsibility for potential privacy infringements become actors in a play between the various parties that together shape the drone. For the drone developer, the drone is just a platform and privacy concerns should be on the side of the designers of smart CCTV (for instance) while the designers of smart CCTV deny their responsibility by indicating that they are unable to predict potential uses of the CCTV and thus to include the values of use in the design.

Policy analysis

The aim of WP3 was to gain a better understanding of how policymakers in Europe conceptualise "security" and privacy in different contexts (national, international, supra-national) and to capture how security and privacy policies are developed in distinct policy contexts, both on the European and Member State levels. It did so by selecting relevant policy documents of European and Member State as well as policy documents from international organisations and the USA and by comparing and contrasting them to one another, in order to identify commonalities and differences between these contexts. Furthermore, insights from WP3 were used to shape the PRISMS survey (in the development of both hypotheses and vignettes).

Deliverable 3.1 of the PRISMS project reviewed policy documents related to privacy and security in the EU, the USA, international organisations, and a sample of EU Member States from 2001 to 2012. Using the search terms “privacy” and “security”, as well as closely related terms and keywords such as “surveillance” and “data protection”, Deliverable 3.1 reported the results of the analysis of 56 documents selected from a long list of 983 documents. The analysis was conducted in two manners. First a Horizontal analysis across the documents, and second a discourse analysis of selected documents around a particular set of key issues.

Drawing upon the stated motivations in the analysed texts the horizontal analysis identified six broad categories of drivers for the compilation and publication of security and privacy texts. These include: 1) responses to legislative requirements, processes or consultation requests, 2) responses to change security contexts or the emergence of apparent new security threats, 3) responses to particular events or identified public concern, 4) reminders or re-affirmations of principles and clarification of laws, 5) the results of scrutiny, inquiry or evaluation of existing policies and programmes, and 6) responses to increased surveillance practices and technological developments. The concepts of security are heterogeneous across different countries, and across different actors within countries. There are multiple, divergent framings of the concept of security, across European governments, and between different policy actors within individual countries. However, many of these concepts are more expansive than the most traditional concepts of national security, and there is an indication that the scope of security has expanded across all countries in the analysis as more areas of social life are represented as contributing towards security. There would also appear to be a relatively stable core of what are considered to be security threats, although with some alterations of priority and some interests specific to individual states. The texts generally value information exchange between security agencies as an important contributor to security. Economic costs of security are rarely if ever mentioned, even in the context of European economic crisis. The concept of national security is expanding in security policy documents across many countries to include information security, often under the rhetoric of cyber security, critical information infrastructure or cybercrime. In a manner similar to the framing of security, these documents provide ways of framing the
problematic of privacy, data protection and surveillance and the appropriate policy, legal, social and economic responses to these issues. The combination of privacy and security documents in this analysis also allows us to reflect upon the way the relationship between the related concepts and practices is presented in public texts. For example, the current EU position on the conflict between privacy and security appears to be that security and fundamental rights (including privacy) are complementary, not in contradiction. Fundamental rights and freedoms are to be “respected” more than “balanced”. The language of “balancing” of privacy and security is however still used at national levels. There are variations across the analysed documents in the representation and use of the concept of surveillance. Different countries have different sets of privacy “threats” – that is, those risks to privacy that are considered to be the most threatening in a particular context. There is a wide and diverse range of privacy problems identified through the documents. These are often shared between countries, but particular issues appear to have increased salience in some countries in comparison to others. There is also a strong thread of technological determinism running through these texts, in which developments in technology have brought about both increased insecurity, but also risks to privacy and data protection. When threats to data protection or privacy arise, they are often portrayed as coming from information technology (such as “databases”) or from information sharing practices, more than from “surveillance” as a phenomenon. Furthermore, there is broad agreement across the texts on the broad principles involved in privacy, data protection and surveillance. These principles include proportionality, accountability, transparency, trust, consent, and the rights of the data subject. The analysed documents indicate also that there may be differences in the solutions and responses put forward in response to particular problems of privacy, data protection and surveillance.

These conclusions were supported by the discourse analysis of selected Dutch, British and EU policy documents. One conclusion of the analysis is that in the past decade, the EU security and privacy discourse had been highly influenced by the 9/11 attacks in the United-States of America (US). In the aftermath of the 9/11 terrorist attacks, the US played a dominant role in the framing of security issues which influenced strongly policies adopted in the EU. The documents examined would indicate that the European Commission found itself several times in the difficult position (to mediate) between the US and the European Parliament (EP) in matters of international cooperation in the fight against terrorism. One of the key storylines emerging from the discourse analysis of documents of the European Parliament is that European citizens’ rights are likely to be violated by the US anti-terrorism measures as these measures would provide the US with disproportionate access to (sensitive) personal data. The dominance of the US in the security and privacy discourse is further revealed by several EU policy documents and EU-US agreements in which multiple metaphors and statements of the US administration(s) are adopted and reproduced in one form or another. In the past years however, the EU discourse on privacy and security appears to have become more balanced with more room for a more rational and in-depth discussion on the security and privacy balance.

The update report Deliverable 3.2 built upon the findings of the first deliverable, and included an updated list of policy documents related to privacy and security published since the first report in March 2013 and the time of writing in February 2015. This report reviewed the key findings and claims made in Deliverable 3.1; identifies 141 new, relevant policy documents; and assesses the findings and claims against a sample of nine of the new policy documents to see if the policy documents published during the study period reflect major changes, a period which coincides with the Snowden revelations about the intelligence
services’ conduct of mass surveillance. As with the previous study, the aim of the review is to provide
insight into the way concepts of privacy and security are used in European and other policy contexts, and
also to inform the survey research and decision support tools to be developed in the PRISMS project. The
second report examined nine key policy documents in detail. For each it provided a summary of the
content and context of the document followed by an analysis in terms of security, privacy, the relationship
between those concepts, technology, surveillance other factors. The update review found some marked
discursive changes between the sample of policy documents included in this updated report when
compared with the policy documents covered by the initial analysis. Whilst some trends remain constant,
there are noticeable changes, which maybe traceable to the Snowden revelations and the resulting public
attention and political fallout. Several of the analysed policy documents serve to open up the rhetorical
space around the concepts of privacy and security. In brief, they do this by exploring the ambiguity of
security (including the increasing prominence of information security as a component part of contemporary
security) and the contingent ways in which surveillance is understood as contributing towards security. In
this context, the traditional opposition between security and privacy is increasingly challenged.

The most substantial difference was the prominence given to the digital mass surveillance. This greater
focus actually allows for a more nuanced, if contested, model of what surveillance (and particularly mass
surveillance) is. Several documents demonstrated the emergence of a narrative of the need for a “re-
balancing” between security and privacy. A new topic emerged in these documents, in part as a response
to the political problem of digital mass surveillance is the extent to which the European Union has any
competency with regard to national intelligence services. The difficulty of achieving accurate
understanding of surveillance and intelligence activities was explicitly raised in several texts. Privacy-
enhancing technologies, and economic and technological methods for increasing privacy and information
security for citizens, even in the absence of a policy or regulatory shift, were the subject of detailed
discussion, whereas these were particularly absent in early policy discussions. Finally, the relationship
between the EU and the US was described in a different, more cautious and potentially competitive
manner.

Criminological analysis

The criminological work package (WP4) contributed in two significant ways to the general remit of the
overall project. The first goal was to arrive to a formulation of a conceptualisation of the notions of security
and privacy from a criminological perspective that could be and were used to provide input for the
development of the survey, its concepts, questions and hypotheses.

The second objective of WP4 was the contextualisation of the results of the survey in light of a qualitative
research case study conducted at Brussels airport, in order to further feed with its insights the
development of the decision support system, one of the final outcomes of the project.

The main goal of this exercise was to explore citizens’ attitudes and evaluations of security. This means
that our leading question is: How do people experience security-privacy practices or situations? To get
insight people’s experiences with security practices we can only rely on how people frame and account
(narrate) these experiences and events. Accounts or narratives are tools that individuals use in a sort of
radical reflexivity connecting actions and accounts. A qualitative case study can precisely focus on the
analysis of accounts or narratives concerning the experience of participants of security practices. That way we can access how participants make sense of the situation they are part of.

Observations were carried out at the security lanes during the months of April and May 2014. In total, the researchers spent 18 hours at the security lanes (Pier A). Observations (20 hours) were also conducted at Pier B (non-Schengen) in the same period as interviews were organised with screeners in the G4S room for personnel located at the Pier B.

The results of this case-study bring us to several reflections relevant for our understanding of how citizens experience and evaluate security practices.

1. Based on the observations, accounts of passengers and of screeners at the security-screening line, we can conclude that there is an overall dominant security logic that requires the almost absolute submission of clients-passengers. As stated before, in this situation of security screening of passengers the security-privacy trade-off has already been settled, in fact it is a condition of possibility for the existing of the dispositive as it exists on the site. Therefore, it is simply impossible for any client-passenger willing to step on his/her flight not to submit. By buying a ticket you are deemed and doomed to agree with the practices of security screening. A first reflection resulting from this small-scale research is that the security screening of passengers has become seen as a “normal” and integrated part of the taking of a civil airplane. Both passengers and screeners voiced this conclusion. Some forms of intimidation and suspicion are thus supposed to legitimately drive and underpin security-screening practices in airports, even if they create some sort of discomfort. Consequently, it is clear that passengers’ security screening, as an everyday airport practice, is already far beyond an effective trade-off between security and privacy. The choice to be made is “to fly or not to fly”, and both passengers and screeners are aware of that. The security line is far beyond the trade-off between privacy and security, if you do not accept to be stripped of your privacy, you won’t pass the security check. An all-encompassing and first line “trade-off” has become part of air travel, and it implies a very high degree of loss at the side of privacy. The only trade off which remains at the line is: a trade off between returning home and pursuing your journey.

2. Therefore, we can easily understand that passengers’ experience of and attitude towards these privacy “invasive” practice(s) is a pragmatic one. That is also the reason why they submit to “the game” of self-disclosure. However, this submission must not be understood as the acceptance of the security-privacy trade-off as such. As described above, it is on the contrary, “spiced” with diverse strategies and small forms of resistance, such as being or behaving as ignorant of the rules, being impervious, discussing the rules, speaking up to security agents. It is within these conflicts that their discontent with the dominant security logic becomes visible. The acceptance of the security line has to do with resignation in the face of a thing to big to contest. It is indeed easier to accept it.

3. The situation of the security screening of passengers can be seen and understood as part of a disciplinary dispositive. By becoming a “natural” or normal part of what airport mobility is about, passengers are nudged and disciplined to meet the ways and ends this routine of security screening is aiming at. The passengers not only are physically channelled and constrained through a sequence of moulds (by human and technological interventions), but also discursively socialised and prepared to the daily practice of self-disclosure (cf. the confession) and made to accept that they have to prove that they
are not suspects (!). You have to behave as demanded - to submit -, otherwise you will remain a suspect and be impeached to catch your flight. The normalisation of such invasive security practices refers directly to Salter’s analysis of the governmentalities of airports. Over time the entire security process, with its different specific security measures, rules and standards, became normalised, and got considered as an integral part of some sort of package deal. At the moment, today, the screeners we interviewed find the body scanner too intrusive, but the potential for normalisation (especially if supported by an implementation on a large scale) and people’s ability to adapt and submit should not be underestimated.

4. The unsettling idea of being treated as a suspect, colours the whole experience: it is heavily present during the screening and is an important source of conflicts. The bottom line is that passengers have the idea that these security practices are set up for others than themselves. The suspects are others, and normal passengers have nothing to hide, which is a standard argument in the security-privacy trade-off discourse. Such implicit assumption refers to a mechanism that can be best compared to the criminological concept of the “criminal other”. Passengers submit willingly to the procedure because they (think they) have nothing to hide. More experienced passengers even cooperate by anticipation. However, it is precisely when they are confronted with some contested rules (cf. bottle of water) or methods (like the selection of their bag or themselves for a more specific control), they re-experience what has been normalised: the position of being a suspect. And that is precisely one of the limits where conflict emerges. Suddenly, they are confronted with the fact that they are and remained, suspects, even if they have nothing to hide.

5. A last and important reflection brings us to what we could call the security paradoxes. From our interviews with passengers, it looks like more information made available on actual threats, on the precise rationale for specific measures and on possible ‘success stories’, along with increased transparency about the decision-making process involved in establishing rules and new measures would. These evolutions are likely to increase people’s willingness to willingly participate in the security control procedures. However, the key point of the whole system is secrecy, as it is assumed that making information freely available would give potential terrorist an edge. Therefore, the specific situation of passengers’ security screening turns into an act that has to be performed, but is emptied of relevant meaning. This, coupled to the recognised illusion of total security through security screening, brings us to an even stronger insight: the security screening of passengers is experienced as a quasi-theatrical and sometimes absurd performance. It has imposed itself as the only possible access to airplane mobility, and as an everyday routine, normalised, boring and a nuisance for passengers. Everybody participates (security agents and passengers) pragmatically by playing the game and to reproduce the expected and chewed discourse when asked. Everybody knows there is no hundred percent security or a zero-risk airplane travel. Doubt is consequently creeping in when the meaning, necessity or usefulness of these practices are at hand. But then, remarkably, it works ... in the sense that citizens just submit to security line controls that would be met with outrage and even active resistance in other settings. And this is unsettling, because the recognition of the illusion of total security operates at the same time as the generator of more and new risks to be detected and fought, leading to more security, and thus again, to more risks.

Legal analysis

Work Package 5 analysed the conceptualisations of security, privacy and personal data protection in EU
law, as well as the relations between them. It provided legal input for the preparation of the PRISMS survey and the interpretation of its results, and for the design of the PRISMS Decision Support System (DSS). Three deliverables encapsulate the work carried out under this WP.

Deliverable 5.1 titled Discussion paper on legal approaches to security, privacy and personal data protection, offers a detailed review of the conceptualisations of security, privacy and personal data protection and their interconnections in EU law. It takes as a starting point that security and privacy are polymorphic notions and have a multiplicity of meanings, not only across different fields and academic disciplines, but also from a legal perspective - and even specifically as components of EU law. In EU law, they now intersect with an additional (perhaps less contested, but possibly not less elusive) legal notion: personal data protection.

The elasticity of the word security, as well as the various nodes of meaning it can denote, are mirrored in the different inscriptions of the term coexisting in EU law, both in its primary and its secondary law. This notably concerns the usage of the term occurs in relation with EU’s external action (one of the EU’s general objectives in its relations with the wider world is to contribute to security) or with the EU’s Area of Freedom, Security and Justice (which has among its main objectives ensuring the safety and security of the peoples of the Member States), as well as its functioning as a limitation of EU primary law, as a ground to restrict free movement, as a key component of network and information security and cyber-security, or regarding the protection of classified information.

Security is actually a word which can refer in EU law to many different types of security, differently related to issues of sovereignty. It can notably allude to security of the State in the sense of the preservation of its integrity, public security as a ground justifying interferences with fundamental EU (market) freedoms, (essential) national security as what is excluded from the reach of EU law, (international) security as pursued by the EU Common Foreign and Security Policy; (EU) security as what is pursued through the Area of Freedom, Security and Justice, and, finally, security interests as grounds justifying interferences with the right to respect for private life and restrictions and modulations of the right to the protection of personal data. Security appears thus somehow as an elastic notion, sometimes moving upwards towards its EU dimension, sometimes retreating back towards its national (or even essentially national) character. Due to this versatility, security takes sometimes the shape of a Janus-faced notion, especially in relation to personal data processing: under its EU light (as an objective of the Area of Freedom, Security and Justice), it supports the proliferation of (EU security) initiatives relying on the systematic processing of personal data, whereas, simultaneously, under its national light (as a prerogative of the State), it justifies (national) restrictions to the provisions that are supposed to mitigate the risks linked to the former.

There exist also numerous legal conceptions of privacy, in particular, regarding its scope, its foundations and its nature. In EU law, its conceptualisation is closely intertwined with the conceptualisation of the respect for private life, an expression for which the word privacy is often used as a substitute - not only in the literature, but also by the legislator. Indeed, in EU law, the term privacy is used primarily to refer to the right to respect for private established by Article 8 of the European Convention on Human Rights (ECHR), nowadays mirrored in Article 7 of the Charter of Fundamental Rights of the EU. Privacy is thus recognised as a EU fundamental right, imported into the EU catalogue of fundamental rights from Article 8 of the
This provision is principally concerned with protecting the individual against interferences by the State, even if certainly not reduced to it (and including for instance positive obligations imposed on the State to prevent interferences by private parties).

The EU Charter of Fundamental rights devotes a specific provision to another right, that is, the right to the protection of personal data, enshrined in the Charter’s Article 8. Until relatively recently, there was some reluctance in the literature to consider personal data protection as a notion fully separate from privacy, and thus to engage in any discussion of its conceptualisation as an autonomous legal concept. The recognition in 2000 by the EU Charter of a fundamental right to the protection of personal data different from the right to the respect for private life was a major stimulus to reconsider such position, even though the legacy of decades of envisioning personal data protection primarily through the frame of privacy is still palpable in most of the discussion around it.

The multifaceted notions of security, privacy and personal data protection inevitably meet in a variety of ways. Although some of their encounters are seemingly unproblematic, it is not always the case. In EU policy and law, major frictions between security, on the one hand, and privacy and personal data protection, on the other hand, occur most often in two specific contexts: first, security can act as a generator of measures potentially encroaching on the fundamental rights to privacy (respect for private life) and to the protection of personal data; second, security can materialise modulating, restricting or limiting the application of such fundamental rights or of the legal instruments that substantiate them.

Personal data protection is therefore recognised nowadays as a EU fundamental right, just like the right to privacy, but it is a right of a different lineage. It has no direct equivalent in any of the classical sources that have led to the determination fundamental rights in EU law: neither in the ECHR, nor in the common constitutional traditions of the Member States. It is thus in a sense a product of the EU Charter, and its emergence has been significantly affected by the Lisbon Treaty. Being a relatively recent right, one could consider that the determination of its substance is normal, but (still) relatively unsettled. What is perhaps more relevant is that its establishment as an EU fundamental right has been structurally linked to a series of peculiar circumstances: it has been “constitutionalised” (in the sense of inscribed in primary law) together with the free movement of personal data across EU law, and with a series of limitations that invite to seriously challenge its qualification as fundamental.

Deliverable 5.2 a Consolidated legal report on the relationship between security, privacy and personal data protection in EU law, studies in detail the conceptualisation and relations of security, privacy and personal data protection in the case law of the Court of Justice of the EU (CJEU), based in Luxembourg, which is the highest interpreter of EU law, as well as in the case law of the European Court of Human Rights (ECtHR), based in Strasbourg, which is the highest interpreter of the ECHR. Together, these two perspectives provide critical insights on how European human rights law envisions the simultaneous safeguarding of security and the fundamental rights to privacy and personal data protection, and thus illuminate the project’s basic inquiry on the validity of the trade-off model as basic frame to understand the relations them.

Ultimately, both the CJEU and the ECtHR support through their case-law a similar, but not identical, vision of the reconciliation of security and privacy (and personal data protection), based on the premise that can only be deemed acceptable the measures that infringe on the rights to privacy and personal data
protection in the name of security that do it in full compliance with a series of requirements, and on the idea that among such requirements stands out the notion of proportionality. The task of identifying concomitances and discrepancies between the two approaches, however, can be rendered peculiarly complex by the fact that in the context of the Council of Europe and in EU law the same terms sometimes operate with slightly different meanings.

This concerns, most notably, the notion of proportionality. In EU law, proportionality can be both understood as a principle applicable to EU action, acting as a limit to such action, and as mirroring the proportionality test devolved by the ECtHR under the expression ‘necessary in a democratic society’. Even in this latter context, regarding requirements applicable to legitimate interferences with ECHR qualified rights, proportionality is generally accepted as referring to two different issues: proportionality in a wider sense would include the requirements of necessity, suitability and proportionality (again), this time understood in a narrow sense or stricto sensu. Complicating things further, such proportionality will depend on whether the measure is limited or not to what is strictly necessary. Additionally, proportionality is also a notion with a specific incarnation in the area of EU personal data protection law, where it can notably act as a fundamental principle underlying all provisions. And, ultimately, courts are always entitled to carry out the test of proportionality as they deem necessary in the case at stake, which typically has been bringing about different approaches and manifestations.

Regarding the validity of the trade-off model, the research shows that for the CJEU, and thus generally for the purposes of EU law, the idea that it is necessary to chose between a legitimate interest and the insurance of fundamental rights such as the right to privacy and personal data protection is not tenable. Such vision was explicitly repudiated by the Luxembourg Court in May 2013 in the Worten judgement, concerning the monitoring of working conditions, and concretely the obligation to always allow for immediate consultation by responsible authorities information relating to the workers’ working time. In that case, one of the parties had argued that the obligation to make available working time information would result in disproportionately giving general access to personal data, but the CJEU asserted that such line of argument could not succeed. Indeed, the CJEU noted that the making available of some information to a certain party had to be implemented while at the same time implementing personal data protection provisions requiring that only those persons duly authorised to access the personal data in question were entitled to process it. It is clear, therefore, that processing personal data for a legitimate purpose does not allow to just generally derogate from personal data protection obligations; on the contrary, these obligations become crucial to effectively delimit interferences with individual fundamental rights.

This fact hints that the ‘security / privacy’ dichotomy must be replaced with a triangular image in which coexist security, privacy and personal data protection. Importantly, this is not a dual picture where security is on one side opposed to (or confronted with, or weighed up against) privacy and personal data protection on the other. On the contrary, the picture that emerges from our analysis is that of a genuinely three-sided relationship, where personal data protection is often called upon to calibrate or mediate potential disparate tensions emanating from privacy or security objectives.

Deliverable 5.3 on The legal significance of individual choices and the relation between security, privacy and personal data protection, investigates the legal relevance of individual choices for defining the relations between security, privacy and personal data protection. Taking ‘law’ primarily as what judges and courts do whenever they rule, rather than legislation, the deliverable is particularly concerned with how
legal decisions are taken using or ignoring individual choices related to security, privacy and personal data protection.

Its underlying assumption is that whenever EU policy makers take security-related decisions they have the obligation to ensure that these are compliant with fundamental rights requirements, but they might also, additionally, be interested in questioning whether individuals would actually perceive such decisions as impacting fundamental rights negatively or not. These are two different issues that cannot be conflated, as one strictly regards compliance with fundamental rights, while the other is about perceptions of compliance. The respect of fundamental rights is unquestionably a legal issue, while perceptions of compliance might be described as a societal consideration, often addressed from an economic perspective and in terms of their possible negative impact on the commercial viability of products.

Individual choices might manifest themselves independently, as a single, personal choice, or in conjunction with other individual preferences. In this case, a sum of individual choices can take the shape of a perceived public opinion, or at least of a certain public opinion, that is, representing the opinion of a certain public. From a conceptual viewpoint, individual choices can be regarded as both reflecting and informing individual preferences. When related to the right to respect for private life and personal data protection, individual choices and preferences might be pictured as globally subsumed under the term ‘privacy concerns’. In this context, it is necessary to keep in mind that individual actions and decisions related to privacy and personal data protection are always multidimensional, and sometimes inconsistent and contradictory. These ‘privacy concerns’ include attitudinal aspects, related to what people perceive, feel and think; cognitive aspects, related to what people know and the information they are provided; and practical or behavioural aspects, related to what people do, particularly in the cases where choice is actually effectively in their hands. All these dimensions are of course interrelated, and influence each other.

All in all, the report documents that the significance of individual choices for defining the relation between security, privacy and personal data protection has multiple facets. Globally speaking, law appears to be ready to fully support personal choices, even those choices that go against of the choices of other individuals, however numerous or persuasive the latter are. It will, for example, decide to ignore some societal opinions that are perceived as going against the basic principles of inclusiveness of democratic societies. Law can also, nonetheless, also pursue the protection of individuals against their own individual choices, and for this purpose reduce or limit the relevance of their preferences.

Against this complex background, the role granted to consent by EU personal data protection law strikes as particularly ambiguous. This ambiguity can manifest in concrete individual decisions, where single acts of consent might appear to go against some established knowledge on the limitations on the waiver of rights. More remarkably, the widespread use and misuse of consent as a ground to process personal data in the EU can also have global consequences when the fact that many individuals appear to ‘consent’ to some popular data processing practices, for instance via the active use of online social media, is taken as evidence of their preferences or lack of ‘privacy concerns’. In a similar vein, policy makers appear to have an increased interest in attempting to appraise the economic value of personal data in the eyes of data subjects, in the understanding that such examination could provide orientation for future policy decision in this area.
In light of these developments, it is crucial to go back to the idea of the multidimensionality of privacy concerns, and to rethink how the limitations imposed by law on the significance of individual choices can be appropriately integrated into their construal. Attitudes, knowledge and practices related to privacy and personal data protection cannot be envisaged as independent dimensions, because they affect each other. From this viewpoint, one should not focus on trying to assess or calculate individuals’ ‘personal’ preferences in relation to the use of personal data concerning them, or to merely take note of how lightly people appear to consent to certain data processing practices, but rather investigate the factors that determine such preferences and practices. In other words, instead of acting as if there were some pre-existing personal choices that happen to operate among the current legal landscape for privacy and personal data protection, it might be necessary to inquire how the current legal landscape shapes current attitudes and decisions, and, finally, discuss which kind of preferences and choices should it encourage or discourage. The exact legal significance of these choices will afterwards, in any case, shift (back) to the hands of courts and judges.

Media analysis

The PRISMS project has 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. In line with the overall project’s research objectives – to explore the relationship between privacy and security and to learn if people actually evaluate the introduction of new security and security-oriented surveillance technologies in terms of a trade-off – the media analysis as conducted in this work package focuses on analyzing the notions of both privacy and security within the European media. As the influence of events on the media’s reporting is crucial, the revelations by Edward Snowden about the mass interception programs from June 2013 are of high relevance for our research. In fact, they mark a disruptive event that was not foreseeable in the beginning of the project and that has the power to change the whole privacy and security related discourse. To take that into account, an additional sample that represents discourse right after the revelations was analyzed additionally. Together with a small sample that was analyzed during the period of media reporting, the results in this report are based on three samples: The initial (2008-2011) and the monitoring sample (2014) for Germany, the UK, the Netherlands, Denmark, Italy and Hungary; and an additional sample for Germany and Great Britain (2013). In the previous report, we had already stated that privacy and security related discourse in Germany, the UK and the Netherlands from 2008 to 2011 is to a vast extent concerned with issues revolving around data and personal information. While the further analyses now show that this proves also true for Italy, in both Denmark and Hungary this dominating cluster of issues was not found. In the same regard, whereas in the other countries discourse from 2008 to 2011 at least partly encompasses a narrative that we chose to call “warning-narrative”, this narrative is absent in Denmark and Hungary. Regarding the notions of privacy and security, although there are variations, there is a tendency of privacy being used most frequently in the sense of privacy of personal data, while security is used more ambiguously. What is different between the different countries is the amount of foregrounding the one or the other – we call it privacy or security-centred. In fact, from the six countries analyzed Germany shows to be the only one where discourse from 2008 to 2011 is clearly privacy-centred, with an emphasis on the risks that the concept is subject to and a strong focus on the need for protection. In the UK, on the other hand, discourse is security-centred. The additional sample that represents discourse directly after Snowden’s revelations reveals that these tendencies stay stable in both of the countries: While in Germany, the focus
is still on the amount of privacy intrusion that became known with the revelations, in the UK the focus on
security – and to be precise, on national security – is even reinforced; although there are variations
between the different sources. Issue-wise, in both countries privacy and security related discourse is
completely reflected in the sense of interception and spying; the affair and its consequences are clearly
dominating. While in Germany, the different sources are quite homogenous in their evaluation of the affair,
the British sources differ; especially The Guardian and The Daily Telegraph. The sample gained during the
monitoring period indicates that the situation is slowly shifting at least partly back to the narratives that
were dominant in the respective countries in the time span before the revelations, but that they are still
reflected in the aftermath of the affair.

Survey results

Descriptive results

Privacy is not dead, as the results of a major telephone survey of more than 27,000 respondents across
Europe has found: 87% felt that protecting their privacy was important or very important to them. Even
more, 92%, said that defending civil liberties and human rights was also important or very important.

The survey may be the most detailed assessment of how people in 27 EU Member States feel about
privacy and security. It was conducted as part of the EU-funded PRISMS project (not to be confused with
the once-clandestine PRISM program under which the US National Security Agency was collecting
Internet communications of foreign nationals from Facebook, Google, Microsoft, Yahoo and other US
Internet companies).

The survey showed that privacy and security both are important to people. There were some consistent
themes, e.g. Italy, Malta and Romania tend to be more in favour of security actions, while Germany,
Austria, Finland and Greece were less so. Respondents were generally more accepting of security
situations involving the police than the NSA.

60% said governments should not monitor the communications of people living in other countries, while
one in four (26%) said governments should monitor such communications, while the remainder had no
preference or didn’t know. Predictably, there were significant differences between countries. Three out of
four respondents in Austria, Germany and Greece said governments should not monitor people’s
communications, which was somewhat higher than most other EU countries.

70% of respondents said they did not like receiving tailored adverts and offers based on their previous
online behaviour. 91% said their consent should be required before information about their online
behaviour is disclosed to other companies. 78% said they should be able to do what they want on the
Internet without companies monitoring their online behaviour. 68% were worried that companies are
regularly watching what they do.

Some other results: 79% of respondents said it was important or essential that they be able to make
telephone calls without being monitored. 76% said it was important or essential that they be able to meet
people without being monitored. More than half (51%) felt they should be able to attend a demonstration
80% said camera surveillance had a positive impact on people’s security; 10% felt it made no difference and even fewer (9%) felt it had a negative impact. Almost three-quarters (73%) said the use of body scanners in airports had a positive impact on security, while fewer than one in five (19%) felt that the use of scanners had a negative impact on privacy. 38% said smart meters threatened people’s rights and freedoms.

More than one in five (23%) said they had felt “uncomfortable” because they felt their privacy was invaded when they were online. Almost the same (21%) felt uncomfortable because they felt their privacy was invaded when a picture of them was posted online without their knowing it. By contrast, a substantial majority (65%) didn’t feel uncomfortable when they were stopped for a security check at an airport. Respondents were asked if they had ever refused to give information because they thought it was not needed. 67% said yes, while 31% said no. Half of all respondents said they had asked a company not to disclose data about them to other companies.

While the survey generally showed that people were concerned about their privacy, there were some surprises. For example, 57% said it was not important to keep private their religious beliefs. Almost one-third (31%) said it was not important to keep private who they vote for. Only 13% had ever asked to see what personal information an organisation had about them. More than half (51%) had not read websites’ privacy policies.

Respondents had a very nuanced view of surveillance and its impact on their privacy. Support or opposition to surveillance depends on the technology and the circumstances in which it is employed, if for example the surveillance activity was targeted and independently overseen.

The interviewers gave respondents eight vignettes, or mini-scenarios, and then asked them for their views on the privacy and security impacts, some of which are highlighted below. The vignettes concerned crowd surveillance at football matches, automated number plate recognition (ANPR), monitoring the Internet, crowd surveillance, DNA databases, biometric access control systems, NSA surveillance and Internet service providers’ collection of personal data.

A sizeable minority (30%) felt that monitoring demonstrations threatened people’s rights and freedoms, but that figure fell to 19% if the monitoring was of football matches. 70% felt crowds at football matches should be surveilled; 61% said surveillance at football matches helped to protect people’s rights and freedoms.

Opinion was more evenly divided about DNA databases: 47% felt that DNA databases were okay compared to 43% who did not agree. However, a substantial majority, 60%, opposed NSA surveillance and 57% felt NSA surveillance threatened people’s rights and freedoms.

Also predictably, there were differences in political views. 68% of people on the left felt that foreign governments’ monitoring people’s communications was a threat to their rights and freedoms, compared to 53% of people on the right who felt this way. 60% said these practices made them feel vulnerable. More
than half (53%) did not feel these practices made the world a safer place. 70% did not trust government monitoring of the Internet and digital communications. In response to a question about how much trust they had on a scale of 0 (none) to 10 (complete) in various institutions, more than half (51%) of all respondents said they had little or no trust in their country’s government compared to 39% in the press and broadcasting media and 31% in the legal system. Half of all respondents had some or complete trust in businesses, and an astounding 70% trusted the police.

Interviewers described a scenario in which parents find out that their son is doing some research on extremism and visits online forums containing terrorist propaganda. They ask him to stop because they are afraid that the police or counter-terrorism agencies will start to watch him. 68% said security agencies should be watching this kind of Internet use, compared to 20% who said they should not. 53% said security agencies’ doing this helps to protect people’s rights and freedoms. One in five (22%) disagreed. 41% of respondents felt that parents should worry if they find their child visiting such websites. One in five felt parents should not worry because they believed that security agencies can tell the difference between innocent users and those they need to watch.

Another vignette concerned companies wanting to sell information about their customers’ Internet use to advertisers. The companies say the information they sell will be anonymous, but 82% of respondents still said service providers should not be able to sell information about their customers in this way. The figure was 90% in Germany and France, the highest in Europe. 72% of respondents in the UK and across the Union felt such practices were a threat to their rights and freedoms.

Analysis of factors influencing citizen perceptions

Our analysis has shown that there is no simple impact of specific factors in the assessment of concrete cases of security technologies and surveillance practices. To answer the research questions on the and to empirically test our theoretical assumptions, we conducted a series of ordered logistic regressions.

The analysis shows that there are only a few factors which play an important role in all cases. Not surprisingly these include citizens’ general privacy and security attitudes. Firstly, in most cases there is a strong positive correlation between worries about personal security and support for a security practice. The support is stronger for the cases of physical surveillance than for virtual surveillance practices, which means that people tend to accept security practices when they come close to personal concerns, are understandable, and do not affect them personally. Secondly, there is an even stronger correlation between privacy worries and the non-acceptance of a security practice.

The third factor that has a significant positive correlation with citizens’ support for a security practice is their trust in institutions. It is clearly visible that the perceived trustworthiness of an authority, organisation, or company operating a security system has a positive effect on citizens’ acceptance. This supports discussions about the importance of trust for the assessment of risks and benefits and the acceptability of technologies. According to these discussions, trust reduces the complexity people need to face. Instead of making rational judgements based on knowledge, trust is employed to select actors who are trustworthy and whose opinions can be considered accurate and reliable. People having trust in the authorities and management responsible for the technology perceive less risk than people who lack that sense of trust in
those members, although some studies seem to suggest that this is not always the case.

Other factors do not show an equally clear picture and are more difficult to interpret, either because the correlations with the assessment of the vignettes are not always statistically significant or even have effects in different directions.

Gender for instance has a significantly positive correlation in three and a significantly negative correlation in four of the cases. Men tend to reject surveillance practices by public authorities more than those of private sector. This is in line with the fact that, according to our survey, men have less trust in public authorities than in the private sector and less trust in institutions in general than women.

Age is an interesting factor inasmuch as it has been recently shown that the younger generation is not generally valuing privacy differently from older citizens. The assumption that this also leads to a more critical assessment of surveillance practices by younger citizens is not supported by the survey results. Rather, the likelihood that young adults (16-34) found a surveillance practice acceptable is higher than that of middle-aged people and much higher than that of older citizens. This correlation, however, is not significant for all the vignettes. Young adults only found the monitoring of websites in search of terrorists a less acceptable practice. Qualitative research by Iván Székely suggests that a possible explanation might be that older citizens, who experienced European authoritarian regimes, are more distrustful, whereas younger people, who had not lived in surveillance states, are less concerned.

In general, the survey has shown that the educational level is positively correlated with the valuation of privacy and negatively correlated with the valuation of security. In concrete cases, however, education only seems to have a weak influence on the acceptance of a surveillance measure. For most of our vignettes one can state that the higher the education level, the less likely it is that one is willing to accept a surveillance practice. This indicates that the more knowledge and understandings of the context people have, the more critical they are. These observations, however, are only significant in some of the cases. This is an interesting complement to the findings about privacy since people with a higher education have a significantly higher appreciation for their privacy than those with an intermediate or low level of education.

It has sometimes been suggested that people living in big cities are more worried about their security and thus more supportive to physical security measures than citizens living in small cities, suburbs, or even in rural areas. Our survey results do not fully confirm this hypothesis. Residents of big cities are only significantly more supportive to the vignette on “school access by biometrics”. Their support for the police use of DNA databases is even significantly lower. For all other cases we could not show a significant correlation. The situation is similarly mixed for smaller cities and suburbs. It is in line with the observation that the people least in danger are most afraid. More important than the fear of crime seems to be the perceived usefulness and effectiveness of concrete measures (Deliverable 4.1).

Political orientation has a weak effect on the assessment. Citizens with a left-wing or liberal orientation are less likely to accept surveillance than those who consider themselves conservatives or right wing.

In summary, one can say that people who are not worried at all about being monitored (do not mind being under surveillance) have lower education, are relatively young, and prefer conservative over liberal thinking.
Our analysis of the questions that aimed to measure European citizens' attitudes towards specific examples of surveillance technologies and practices had the following main results:

* Trust in the operating institution is an essential factor for the acceptance of a surveillance-oriented security technology

* Openness has a positive effect on the willingness of citizens to accept security practices. This can be understood on different levels:
  -- The surveillance activity should not be covert but perceivable for the citizen.
  -- Citizens tend to accept security practices when they are addressing their personal concerns. Thus, they need to be convinced that a security measure is necessary, proportionate, and effective. A nuanced and critical view on them is also a question of proper education.

* On the downside it can be stated that many citizens do not care about surveillance measures that do not negatively affect them personally.

Decision support system

Work package 11 aimed to bring together the investigation of concepts of privacy and security into a decision support system (DSS) that guides those who aim to deal with a security threat and help them to explore solutions that minimize the impact on the privacy of individuals while achieving the security objectives. DSSs are tools that aim to support and guide decision makers in the process of making complex decisions and that are based on data and decision-making models. They offer flexibility in the decision-making approach and they can be used by experts and non-experts alike.

In comparison with the majority of other work packages in the PRISMS project, the work conducted under WP11 was largely a design, testing and evaluation process which drew upon the research conducted in the rest of the project. As a result it has a product (The DSS itself), and also more diffuse findings that can be extracted from the design process itself. It was therefore an iterative process, with several design cycles, particularly significant stages of which are captured in the work package deliverables. This design process also fed into the consideration of D10.3 which examined the potential dual-use of the PRISMS DSS. This had been a concern through the design process and several design elements of the DSS are intended to minimise the risk of unwarranted use.

The approach of the PRISMS DSS is normative; it has an explicit ethical goal of minimizing the impact on the privacy of individuals of any kind of security measure. This DSS provides insight into the pros and cons of specific security investments compared to a set of alternatives taking into account a wider societal context. This means that the PRISMS DSS specifically takes into account a wider perspective than just that of the problem owner or the stakeholder responsible for making the security investments. The assessment made by the PRISMS DSS is a comparative assessment, in which alternatives are weighted against each other. The DSS is based upon a perspective that is rooted in well-known impact assessment methodologies. Instead of the privacy-security trade-off perspective we adopt an approach in which security and privacy are considered to be separate dimensions with their own value schemes that need to be weighed against each other in an integrative approach. In this manner PRISMS intends to overcome the simplistic assumption that one cannot have both security and privacy when offering safety measures or implementing security devices.
This work package has therefore produce a usable decision support system based upon a document & template approach. A decision maker proceeds through a set of templates, answering questions in those, bringing in additional information as appropriate, including third party perspectives and information from other studies (including the PRISMS survey and information from other work packages). At the end of this process, the decision maker will have conducted a structured comparison of alternative security measures in relation to a clearly specified security problem. The DSS is designed to highlight and draw out the multiple privacy, fundamental rights and data protection issues that can arise from the implementation of security technologies, and make these accessible to the decision maker, allowing for a meaningful comparison.

Deliverable 11.1 - Towards a PRISMS Decision Support System presents background information on the DSS as this had been developed in the PRISMS project and presented a first version of the templates to be used within the DSS. The background information is meant to help those that will use the DSS and its templates for discussing and deciding upon security issues. It also sets out the concepts of privacy and security as they have been developed in PRISMS, the guiding principles for the DSS, the anticipated audience for the DSS, as well as initial guidelines for use.

This report captures a design process in mid-flight. Taking into account the generic principles behind deploying design science, this design science process developed the DSS in three subsequent steps. Firstly, all conceptual information that can be used to guide the development and design of the DSS has been gathered and formulated as (functional) requirements for the system. Secondly, the actual DSS was designed and developed. This stage again consisted of three steps. Firstly, the decision-making process has been defined and elaborated, distinguishing different steps. Secondly, based on the decision making process, a functional design of the DSS has been created that supports the different steps of the decision-making process. This functional design consists of formulating all the building blocks that make up the DSS, as well as the links between these building blocks. Furthermore, within the DSS a number of templates have been identified and subsequently elaborated that are used for information gathering and analysis. Both the overview of the building blocks and the elaborated templates have been designed in this phase. Based on the results of these efforts, the third step of this stage is the creation of a tool that functions as a guide to the assessment process. This is a tool that may contain questions and a routing through the questions. The aim of this tool is to help those that want to use the DSS. The report also contains the analysis conducted by the PRISMS DSS team on a number of other recent design support systems with security relevance. This review exercise enabled the team to better understand what was feasible in the DSS design space, and to learn from existing DSS as well as those currently under development.

The WP necessarily engaged with the tensions between the emergent and theoretical model of the relationship between the concept or privacy and security coming from PRISMS research, the possibilities of manifesting those findings in a DSS, whilst at the same timing creating a DSS that was usable, and offered something to potential users. It required developing a working model of security decision making (including its flaws) in order to design a DSS that could adequately support and integrate into this, whilst at the same time meeting the normative commitments that arose from the concepts of security and privacy in PRISMS.
Deliverable 11.2 - Evaluation of the DSS by use cases documents the testing of this prototype version of the PRISMS DSS (as set out in D11.3) in two case studies. The cases included a security technology and context where privacy is at least potentially impacted, the two different contexts allowed for comparison. The first use case was a real use case. The Vrije Universiteit Brussel (VUB) intended to introduce a new electronic key system that provides access to the campus, to buildings and to specific locations within buildings. The VUB considered the PRISMS DSS an interesting opportunity to discuss potential privacy implications of the new system, taking a role as responsible actor towards this innovation, and helping to test the feasibility of the DSS at the same time. The second use case had to be constructed by the project team. The case constructed was the introduction of smart CCTV (as compared to 'ordinary' CCTV) at a fictitious airport in order to track terrorist activities before a sincere terrorist attack occurred at the airport. Both case studies produced findings that fed back into the design of the DSS. The goal of the DSS is to include privacy and data protection as constraints and values in the decision process, whilst considering other values (such as cost efficiency) as well. The DSS being a supportive system (not making the decision itself) should focus on bringing into perspective the pros and cons of the security measures, the limits and constraints and the wider societal context. Different alternatives need to be assessed on their performance regarding these conditions and the results should be presented in a manageable overview that supports the final decision for a specific solution. Due to the approach taken in the second case study (focusing more on the methodological approach taken by the DSS as opposed to the specifics of the case itself) the workshop proved to be most productive in producing information on the approach of the DSS. The workshop highlighted issues around questioning assumptions of security decision makers, that going beyond data protection principles was appreciated, and highlighted the potential role of the DSS (or elements of it) in future privacy impact assessment requirements. Several questions raised by workshop participants had already been dealt with in parts of the DSS approach, but we were not able to demonstrate these in the short session. The workshop also highlighted issues with involving security investors and provided suggestions on how to target potential users. In response the DSS was adjusted to include additional elements.

Deliverable 11.3 contains the PRISMS DSS approach: a document based-process for the systematic consideration of security and privacy in a security investment decision, including participatory elements. The document starts with the basic principles of the DSS, and guidance on the intended audience and intended use. It then provides guidance on using the DSS approach in three contexts: 1) a self-directed approach where a decision maker (the "security investor") works through the questions and templates of the DSS, either by themselves, or with a small internal team in order to structure their own analysis of a security investment decision, 2) a focused approach to structuring exploratory interactive sessions for generating new ideas and perspectives which can feed into security decisions, and finally 3) a comprehensive approach using all the resources of the DSS to fully support the security investment decision. The document contains templates to be used in each stage of the process, and provides annexes containing additional resources. The report is formatted so that it could be used as a complete DSS itself. The report is supported by an excel-based spreadsheet tool, which provides a way of approaching and managing the templates, as well as some supporting features (such as automatically populated fields). The system itself does not function as a stand-alone tool that can be used off the shelf. It needs involved people who understand the structure of the tool, the structure of the DSS and the various steps that need to be taken.
The DSS consists of the following stages. A Preparatory phase focused upon preparing the material for the assessment phase. It is composed of a number of building blocks that starts with getting a proper view of the threat that needs to be countered. It continues with inventorying the security measures that are proposed to counter the threat. Special attention is given to what is known about the effectiveness of these measures. Alternative measures are sought for. These measures should be genuine alternative measures, meaning that they are sufficiently mature and robust to offer a realistic alternative to the security measures as originally proposed. For all measures available evidence will be collected on various aspects of the measures (effectiveness, acceptability by involved citizens, costs). The Assessment phase starts with assessing the potential infringements of fundamental rights. This relates to legitimacy, suitability and necessity of the measures proposed. To indicate a serious drawback, red flags are used in this phase. The second step is an assessment of the privacy implications. Finally, the assessment inventories how affected persons/groups of persons perceive the impact of security measures. In the third phase, Mitigation the negative consequences that have surfaced will be checked for opportunities to mitigate them. A first check will be done on whether the measures proposed are open for mitigation, and whether they contain red flags that might be prohibitive for the measure as such. Then it will be checked what kind of mitigation measures can be used to improve the measure. The final phase is the Reporting phase in which all elements that have been gathered will be presented. The presentation starts from the requested analysis: pros and cons, constraints and limitations and the wider social context. Finally, a management summary will be produced. During all phases, stakeholder consultation (in the form of working group meetings, conferences, focus groups, interviews, surveys, etc.) can be part of the approach.

Potential Impact:
In summary, the research conducted in the PRISMS project has led to the publication of three edited volumes (including the forthcoming final conference proceedings), one monograph, eighteen peer-reviewed journal publications, nineteen book chapters, six workshop panels organised by the consortium, a final conference attended by 140 people, thirty-three presentations at third-party events, liaison and interaction with twenty-five different EU and national research projects, and twenty-one press articles, as well as informing a submission to a parliamentary inquiry. At the time of writing this report there are still some articles in preparation or under review and these are likely to emerge in the coming months.

Research emerging from the PRISMS project has, we believe, been well disseminated into the academic community, with the consortium partners producing a large number of academic journal articles, book chapters and the like, and presenting research from PRISMS to a range of academic forums. There are several more articles under review or in preparation and dissemination of this type can be expected to continue over the following year. These publications are being cited and built upon by other researchers in the field. The liaison activity with other projects demonstrates how PRISMS engaged in this research community.

PRISMS press and media dissemination activity in many ways sits in the shadow of the Snowdon revelations. Privacy is clearly a topic that does attract media attention, as evidenced in PRISMS deliverables D6.1 and D6.2). However, whilst there has been increased media attention to topics of privacy and security over the lifespan of the project, this has had some unexpected impacts. We experienced that many news outlets who had focused upon surveillance-related stories felt they had sufficient material on these topics, particularly as new revelations emerged, and that the findings from a
research project were less newsworthy than ongoing political events.

The dissemination of the PRISMS survey results into this environment has been complicated by the survey design. The PRISMS survey design was appropriately intended to counteract some of the methodological problems with existing survey work on privacy and security attitudes (as detailed in Deliverable D7.1 - Report on existing surveys). The focus was less upon the headline descriptive statistics, as are common in many other surveys, but rather about finding more durable, longer term insight into the factors that influence perceptions and attitudes regarding privacy and security. As a result the survey results required careful and time-consuming analysis. Secondly, the survey results began to emerge in the crowded context of several other surveys about privacy, security and surveillance. The PRISMS survey data set will be made available in several appropriate data repositories in order to maximise access and secondary analysis by other interested researchers.

The PRISMS Decision Support System has been finalised at the tail-end of the project and this will be disseminated through a targeted promotional campaign to security industry and public sector associations, as based upon the findings in the validation process, these areas offer the best opportunity for up-take of the system. The DSS material and supporting documentation will be made available through a dedicated section on the PRISMS website. It is hoped that this system will contribute towards the growing field of impact assessment methods and tools in this field.

List of Websites:
http://prismsproject.eu/
Dr. Michael Friedewald, michael.friedewald@isi.fraunhofer.de (co-ordinator)

Last update: 14 November 2016
Record number: 191772

Permalink: https://cordis.europa.eu/project/id/285399/reporting

© European Union, 2022