Project acronym:	SAPIENT
Project title:	Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies
Project number:	261698
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2010.6.5-2: Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules
Contract type:	Collaborative project
Start date of project:	1 February 2011
Duration:	42 months

Deliverable 5.2
Final Report: Findings and Recommendations

Editors:	David Wright (Trilateral Research & Consulting); Michael Friedewald (Fraunhofer ISI)
Contributors:	David Wright, Inga Kroener, Monica Lagazio, Rachel Finn (Trilateral); Michael Friedewald, Dara Hallinan (Fraunhofer); Raphaël Gellert, Rocco Bellanova, Serge Gutwirth, Matthias Vermeulen (VUB-LSTS); Marc Langheinrich (University Lugano)
Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Due dates:	30 July 2014
Submission date:	25 July 2014

About the SAPIENT project

The SAPIENT project that is expected to provide strategic knowledge on the state of the art of surveillance studies, emerging smart surveillance technologies, and the adequacy of the existing legal framework. In addition to addressing these core research goals, the project will entail the development and validation of scenarios around future smart surveillance systems, and will apply the best elements of existing PIA (privacy impact assessment) methodologies to construct a surveillance related PIA framework.

The work of the project will lead to a practical handbook which will help policy makers, technology developers and other stakeholders to better understand how and when smart surveillance should be used, and apply criteria to assure that such systems respect the privacy of citizens.

Terms of use

This document was developed within the SAPIENT project (see `http://www.sapientproject.eu`), co-funded by the European Commission within the Seventh Framework Programme (FP7), by a consortium, consisting of the following partners:

- Fraunhofer Institute for Systems and Innovation Research (co-ordinator),
- Trilateral Research & Consulting LLP,
- Vrije Universiteit Brussel,
- Università della Svizzera italiana,
- King's College London, and
- Centre for European Policy Studies

This document is intended to be an open specification and as such, its contents may be freely used, copied, and distributed provided that the document itself is not modified or shortened, that full authorship credit is given, and that these terms of use are not removed but included with every copy. The SAPIENT partners shall take no liability for the completeness, correctness or fitness for use. This document is subject to updates, revisions, and extensions by the SAPIENT consortium. Address questions and comments to: `feedback@sapientproject.eu`

Document history

Version	Date	Changes
1.0	22 July 2014	

Contents

1 Introduction

This Final Report of the SAPIENT project summarises the key findings and recommendations of previous deliverables. While preparation of the report was largely a matter of extracting the key findings and recommendations from previous deliverables, the consortium has taken the opportunity to re-examine our initial findings and recommendations and, if necessary, to update them, particularly in the context of the Snowden revelations, which began 5 June 2013, and the European Court of Justice's ruling in April 2014 that the EU Data Retention Directive was invalid, as it interfered unduly with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

The aim of the SAPIENT project was to provide for policy-makers, developers of surveillance technology and other stakeholders strategic knowledge on the state of the art of surveillance studies, emerging smart surveillance technologies and the adequacy of the existing legal framework. The consortium developed scenarios around future smart surveillance systems for discussion with focus groups of stakeholders aimed at providing a consolidated analysis of stakeholder views on the use of surveillance.

The consortium adapted a privacy impact assessment framework to address the particularities of smart surveillance systems, technologies, projects and policies. To that end, it extracted the best elements of existing PIA methodologies in order to construct a surveillance-suitable PIA framework (i.e., a surveillance impact assessment (SIA) methodology), which it tested on three different surveillance projects, the first time this happened at European level. It then derived lessons learned to refine its proposed methodology and to present its results at a final conference and in a final report together with its recommendations.

2 Five insights to inform impact assessments

A state-of-the-art review of smart surveillance[1] offered five key insights for the study of smart surveillance and the reflection on how an innovative privacy impact assessment methodology tailored for surveillance can be devised.

The second point concerns the relation between surveillance and freedom. Surveillance is no longer correlated solely to a disciplinary logic that entails a vertical exercise of authority. Surveillance practices currently stand in relation to a logic of normalisation: they operate through freedom, rather than in negation of it. The image of a "balance" between security/surveillance and freedom cannot be considered as an adequate representation of the policy challenges involved in devising privacy-oriented methodologies.

Third, the main area of concern regarding contemporary surveillance trends is the generalisation of dataveillance. However, the use of electronic data should not be regarded just as an enhancement of previous surveillance practices. Dataveillance is used for profiling and in security policies for prevention and apprehension of crime and terrorism. This trend

[1] Gutwirth, Serge, Rocco Bellanova, Michael Friedewald, et al., "Smart Surveillance - State of the Art Report", Deliverable 1.1, SAPIENT Project, 2012.

towards prediction and its corollaries, including the increasing reliance on data-mining and the processing of “bulk” data, should be placed at the forefront of discussions on privacy.

Fourth, surveillance is not a homogenous process. The politics of surveillance involve various forms of resistance, combining collective and individual attitudes. In some cases, surveillance may be considered as desirable, or will call upon the active participation of individuals. Surveillance is thus dynamic and evolves through struggles and controversies. While important, privacy and data protection should not be considered as the only ramparts against surveillance. Privacy and data protection operate in relation to other rights that might be challenged by surveillance, and in broader social configurations that are dynamic and changing.

Finally, the analysis of “smart surveillance” and the correlated devising of an SIA methodology should embed the more technical aspects of this discussion with an overall analysis of the legal and political struggles unravelling around the issue of surveillance.

3 Smart assemblages

Current and emerging technologies are increasingly being organised into assemblages or “smart surveillance” systems, where surveillance systems are becoming integrated, multimodal, automated, ubiquitous and increasingly accepted by the public. Contemporary surveillance involves different technologies and is used in different settings, for a range of purposes. In addition to more traditional criminal justice and national security applications, surveillance technologies, and often systems of surveillance technologies, can be found in public spaces, mass transit, air travel, consumer space and combined with technologies or systems associated with communication and entertainment. As individuals travel back and forth to work or on errands, shop in-store or online, visit their town centre, communicate with friends and family, watch television, go on holiday, surf the Internet or even go for a hike near national borders, they are often subject to surveillance by a range of systems. As such, surveillance technologies have become part of our daily infrastructure and part of the quotidian activities that we undertake on a day-to-day basis. Such surveillance has “enter[ed] our daily life without notice, [and] become a common part of our socio-political and economic relations, so that we become acclimatised or accustomed to surveillance”.[2] The SAPIENT consortium investigated how emerging forms of surveillance are becoming pervasive in our daily lives and by examined the public’s acceptance of different forms of surveillance. The Snowden revelations have confirmed our worst fears about the pervasiveness of surveillance. The public’s reactions to those revelations – some appalled, some accepting such pervasiveness as necessary to fight crime and terrorism – have shown that neither public acceptance nor public rejection can be taken for granted.

Existing and emerging technologies are becoming “smarter”. Many existing surveillance systems, particularly systems that involve verification (biometrics to enable access to controlled spaces), detection and monitoring (sensors that detect explosives or other prohib-

[2] Wright, David, Michael Friedewald, Serge Gutwirth, et al., "Sorting out smart surveillance", Computer Law & Security Review, Vol. 26, No. 4, 2010, pp. 343-354, [p. 344].

ited items) or information linking (credit scoring), already often involve automated decision-making and can be aggregated to identify general trends, or scaled to the level of an individual, or set of individuals, of interest. Automation is a particular goal of many surveillance-related research initiatives of both the EU Seventh Framework Programme and the US Defense Advanced Research Projects Agency.[3] This trend indicates that humans are increasingly relegated to the role of second-level decision-makers, with a range of potential discomforts and negative impacts for individuals subject to these systems. Integrated, multi-modal systems are increasingly becoming a feature of current and emerging surveillance technologies. Currently, biometrics requires the existence of both biometric measuring algorithms and databases or other back-end computing systems to store and recall data. Similarly, unmanned aerial vehicles (commonly known as drones) themselves are not useful for surveillance until they are fitted with cameras, sensors or other technological devices. Emerging research initiatives and technologies are set to continue this trend with systems integrating analytical algorithms with video surveillance, developing mobile sensor networks and so on.

Surveillance is becoming increasingly ubiquitous, integrated and more powerful, a fact confirmed by the Snowden revelations. There is no doubt some surveillance yields social benefits, but equally there is no doubt that those controlling surveillance systems gain more power over those surveilled and targeted. Benjamin Goold speaks of the political dangers of surveillance and counsels that "[w]e should resist the spread of surveillance not because we have something to hide, but because it is indicative of an expansion of state power. While individuals might not be concerned about the loss of autonomy that comes from being subjected to more and more state scrutiny, it is unlikely that many would be comfortable with the suggestion that more surveillance inevitably brings with it more bureaucracy and bigger, more intrusive government."[4]

4 A legal analysis of fundamental rights in the context of smart surveillance

The SAPIENT consortium developed a legal analysis of fundamental rights in the context of smart surveillance. Its goal was to advance a state of the art to pave the way to further analysis and research. It proposed seven elements, or points of reflection, to advance beyond this first move.

4.1 Smart surveillance and data minimisation

Calling a measure 'smart' might raise the expectation, from a legal point of view, that a measure will be targeted to a specific individual, thereby reducing adverse effects on others. This interpretation of 'smart' correlates with the principle of data minimisation, i.e.,

[3] Gutwirth, et al., 2012.

[4] Goold, Benjamin J., "Surveillance and the Political Value of Privacy", Amsterdam Law Forum, Vol. 1, No. 4, 2009, pp. 3-6, [p. 5].

that as little data as possible should be actually gathered. Hence, data minimisation should not only affect smart surveillance at the moment of data collection, but also its core data processing features, which should be able to generate knowledge out of a limited data set. Such a possible conceptualisation of smart surveillance seems particularly promising from a human rights perspective, as it would dramatically reduce its possible negative impact. However, two caveats should be taken into account. The first concerns EU policy trends, an example of which is the Commission's support for the principle of data minimisation, as reflected in the proposed Data Protection Regulation.

The second caveat is based on an analogy with 'smart sanctions'. Smart sanctions (such as the freezing of assets or imposing of travel restrictions) against certain individuals or groups were originally introduced by international actors such as the EU and the UN as a response to the criticism that sanctions against states, for instance, through trade restrictions, were a too blunt instrument that affected the humanitarian situation of complete populations.[5] While such smart sanctions indeed stopped the general suffering of these populations, they did not turn out to be a panacea to pressure repressive regimes into accepting change. Various reports have shown how targeted sanctions have been characterised by severe due process concerns (in the case of terrorist listings, for example) or cases of mistaken identity on the basis of wrongly spelled names.[6]

4.2 Scalable data gathering

Some surveillance technologies can be transformed into 'smart' ones by the adoption or inclusion of specific features. For example, from a fundamental rights perspective, neither body scanners nor smart CCTV cameras, for instance, store data until the system notices a 'dangerous' object or a dangerous 'situation'. As such, these smart surveillance techniques are, therefore, perceived as a form of tailored surveillance, in which data gathering is somehow scalable: stand-by observation without ongoing retention of data or, in the case of advanced body scanners, generation of personal data. An operator working at an airport, in a CCTV control-room or near a body scanner will only be interested in an individual when the system signals that 'something is wrong'. This leads easily into thinking that persons who don't trigger the pre-defined alerts of these smart surveillance systems won't be affected by their use, which, consequently, does not amount to an interference with their rights. Two elements should nevertheless be highlighted. The first concerns the productive effects of data protection on this evolution. For example, in the case of body scanners, it can be argued that the 'smart' technological solutions lately proposed have been a sort of response to data protection institutional and legal mechanisms. The second element concerns the issue of 'mere' data retention: when data are not always subsequently processed. Indeed, the European Court of Human Rights has made clear that the fact that information is only gathered and not always subsequently used in practice, is irrelevant for the application of

[5] See for instance, Cortright, David and George A. López (eds.), Smart sanctions: targeting economic statecraft, Rowman & Littlefield, New York, 2002.

[6] Cameron, Iain, "Report to the Swedish Foreign Office on Targeted sanctions and legal safeguards", 2002.

Article 8 of the European Convention on Human Rights (ECHR).[7] Therefore, it represents in itself a form of intrusion in the private life, which should be assessed according to the test established in Art. 8(2) ECHR.

4.3 Machines operated surveillance: automatic non-discrimination?

Another advantage, theoretically, seems to be that there is no risk of discrimination in using smart surveillance techniques, since it is the machine that selects persons for further investigation, and not an operator. In the case of body scanners and smart CCTV cameras, no decision with a negative effect is taken without further verification by an operator. Smart surveillance technologies only help the operator to focus his attention on persons to whom – according to the machine – appear to be of interest. Recital 20 and Article 3(5) of the European Commission's Passenger Name Record proposal similarly provide that no enforcement action shall be taken by the Passenger Information Units (PIUs) and the competent authorities of the Member States solely on the basis of the automated processing of passenger name record (PNR) data.[8] In other words, smartness is performed by a re-distribution of roles between machines and human operators. Machines should ensure that the first shift is not biased by prejudices, then, the (same) human operators who were initially sidelined are supposed to guarantee a fair judgement of the 'anomalies' spotted by machines. Such a rationality can foster the idea that surveillance by machines, which have a much greater surveilling capability compared to humans, is, by default, less discriminatory, and therefore their use should be further extended in order to compensate for human prejudices. This does not mean, however, that no discrimination concerns arise. The idea that machines by definition enforce "neutral" criteria is misleading.[9] Since their 'nature' cannot be presented as a guarantee against discrimination, their operations, and their interactions with other elements, should equally be the object of a series of controls, including ex-post checks, to ensure that discrimination is not taking place. In this sense, human verification is just an instrument, and not the definitive solution. Rather, the use of statistics proposed by the Fundamental Rights Agency in its 2011 EU PNR opinion[10] could become an important step to ensure oversight on the entire surveillance process.

[7] "The storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding." See Leander v. Sweden, 26.03.1987; Kopp v. Switzerland, 25.03.1998; Amann v. Switzerland, 16.02.2000.

[8] A comparable provision has been included with regard to the tasks of the competent authorities in Article 4 (6).

[9] Kranzberg, Melvin, "Technology and History: "Kranzberg's Laws"", Bulletin of Science, Technology and Society, Vol. 15, No. 1, 1995, pp. 5-13; Albrechtslund, Anders, "Ethics and technology design", Ethics and Information Technology, Vol. 9, 2007, pp. 63-72.

[10] European Union Agency for Fundamental Rights, "Opinion on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final)", FRA Opinion 1/2011, Vienna, 2011.

4.4 A comprehensive data protection framework and private-public surveillance partnerships

The development and use of smart surveillance technologies coincides with a major reform of Europe's data protection rules. The most important revision is the revision of the Data Protection Directive, and some relevant trends in the review process are of particular importance to smart surveillance technologies. The potential adoption of a comprehensive framework (as proposed by the European Commission in the prospective Data Protection Regulation of 25 January 2012 and as adopted by the European Parliament in its version of April 2014) is a welcome development in the provision of the EU with a consistent data protection framework.[11] Such a framework would in particular be helpful for solving the seemingly inextricable legal PNR-knot, but it is very relevant for the other smart surveillance techniques as well. Not all operators of smart CCTV cameras or body scanners resort under the law enforcement sector in certain Member States; a comprehensive legal framework will help to overcome the uncertainty that is a result of blurring activities of the private sector and of the law enforcement sector. The comprehensive framework set out in the EC's reform package of 25 January 2012 is likely to act as a counter-balance against the current overstretching of the purpose limitation principle in the former third pillar as well. However, one should keep in mind that the European Commission proposed the Regulation in conjunction with a Directive concerning the processing of data for law enforcement purposes.[12] Conflicts of scope are therefore likely to subsist, not least as far as the regulation of profiling and data mining is concerned, as both texts address profiling but fail to do so for data mining.[13] Furthermore, the latter does not explicitly mention the data minimisation principle.

4.5 The notion of personal data

The use of smart surveillance technologies shows more and more the limits of the notion of "personal data". Unfortunately, in the proposed Regulation, the Commission has made no more precise definition, beyond its generic commitment to "ensure a coherent application of data protection rules, taking into account the impact of new technologies on individuals' rights and freedoms".[14] The proposed Regulation sets out the measures that a state should

[11] At the time of preparation of this SAPIENT Final Report (July 2014), the European Council has not yet reached an agreement on the proposed Regulation.

[12] European Commission, "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offencesor the execution of criminal penalties, and the free movement of such data", COM(2012) 10 final, Brussels, 2012; European Commission, "Impact Assessment Accompanying the General Data Protection Regulation", SEC(2012) 72 final, European Commission, Brussels, 2012; De Hert, Paul and Vagelis Papakonstantinou, "The Police and Criminal Justice Data Protection Directive: Comment and Analysis", Computers & Law Magazine of SCL, Vol. 22, No. 6, 2012, pp. 21 - 25.

[13] Currently (as of July 2014), profiling is defined (in Article 4) of the proposed Data Protection Regulation. Data mining, however, is not addressed. The same holds true for Art. 9 of the proposed Directive.

[14] European Commission, "A comprehensive approach on personal data protection in the European Union", COM(2010) 609 final, Brussels, 2010, [p. 6]; European Commission, "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the

deploy to protect the 'legitimate interests' of a person, including by specifying which possibilities exist to lodge a claim for damages if the use of data processing by governmental organisations is in breach of Article 8 ECHR or other human rights.

The proposed Regulation may have effects on the evolution of surveillance systems, for example, by pushing for the use of limited amounts or limited sets of personal data. However, the paradoxical risk of some of these developments is that data protection loses its ability to apprehend them when data are not considered "personal". Therefore, more reflection is needed on how to maintain data protection as relevant as well as other types of privacy (which are not at all covered by the proposed Regulation) in the face of specific technological developments.

4.6 Effectiveness

The German Constitutional Court ruled in 2006 that the use of a 'preventive' screening method towards a person would only be compatible with the proportionality requirement if it were shown that there was a 'concrete danger' to national security or human life, rather than a general threat situation, as it existed since 11 September 2001.[15] If we apply this threshold to the use of body scanners, smart CCTV and PNR, it would be hard to say in general that there is now more need for these technologies. Furthermore, this lack of clarity concerning 'concrete dangers' is often mirrored by the inability to assess the effectiveness of specific measures. This is an important issue, as effectiveness is an important element of the proportionality test, and 'blank cheques' are not an option in the field of surveillance. Still, many of these proposed systems are highly dubious in terms of their outputs. Since there are an infinite number of risks and only a limited (if not shrinking) amount of resources to spend, priority should be given to those that ensure an added value in terms of effectiveness. It is therefore crucial that any adaption of 'smart surveillance' systems is accompanied by a proper impact assessment that examines not only the societal and fundamental rights impact, but also the economic impact of such a measure.[16]

4.7 Has privacy been left behind?

Most of the legislative attention on the European level is devoted to improving the rules and legislation regarding data protection.[17] Privacy is often only mentioned en passant, and is not explicitly taken into consideration. 'Traces' of privacy remain, at least nominally, in such practices as 'privacy by design' and 'privacy impact assessment' (although in the proposed

Regions. A comprehensive approach on personal data protection in the European Union", European Commission, Brussles, 2010, [6].

[15] BVerfGE 115; 320, "Rasterfahndung II", 4 April 2006.

[16] Maras, Marie-Helen, "The economic costs and consequences of mass communications data retention: is the data retention directive a proportionate measure?", European Journal of Law and Economics, Vol. 33, No. 2, 2011, pp. 447-472; Kreissl, Reinhard, Clive Norris, Marija Krlic, et al., "Surveillance: preventing and detecting crime and terrorism", in Wright, David and Reinhard Kreissl (eds.), Surveillance in Europe, Routledge, London, New York, 2015.

[17] Wright, David and Charles Raab, "Privacy principles, risks and harms", International Review of Law, Computers & Technology, Vol. 28, No. 3, 2014.

Data Protection Regulation, these have become data protection by design and data protection impact assessment, which are narrower concepts), and in the generalisation of the lawfulness test, which builds upon Article 8(2) of the ECHR. But privacy is more than the protection of personal data. This observation is not only interesting for academic purposes, since it raises the issue of how to make full use of two distinct (even if overlapping) rights, and of how to articulate them to offer a better protection. Indeed, in the case of the full implementation of the proposed Data Protection Regulation, the right to data protection cannot be assumed to be the only tool in dealing with smart surveillance practices. Many threats could be avoided via an expansion of data protection, not only in terms of policy areas or reach of rights, but also in terms of scope over the elements of the security assemblages, explicitly including human and non-human ones. However, future research needs to put more attention to the evolving role of the right to privacy in a technology-driven 21st century, resisting the temptation to fully conflate it into the right to, and the legislation on, data protection. Such an effort is probably essential in order to assess the legitimacy of smart surveillance technologies, since a re-assessment building upon the right to privacy could render legal smart surveillance tools (from a data protection point of view) illegal in a not so for away future.

5 Public opinion

Privacy and data protection are highly complex concepts around which public opinion is diverse, fluid and strongly tied into a series of other issues. However, certain trends are evident. Key amongst these is that the public perceives the right to privacy in a somewhat unbalanced way, preferring its individual importance over its social function. This leads to a similarly unbalanced weighing of importance in relation to other social issues. The complexity and invisibility of the data environment makes it difficult for the public to perceive surveillance trends and structures.

Surveys exploring surveillance as a practice and as a technology represent a complex field. While most surveys report levels of support from different publics for surveillance measures to ensure security as a response to threats, those that interrogate this or that explore particular practices or surveillance technologies reveal a more nuanced level of public acceptances.

When considered alone or as part of wider assemblages, the technical capabilities of surveillance technologies are not often understood whilst in their presentation, the terminology is mixed and uncertain and the boundaries of discourse around and between technologies are fluid. As a consequence, the public has difficulty in forming images of the technologies themselves or of locating their relevance in wider and equally complex social debates. It is thus difficult to evaluate what they mean. Whilst surveillance technology may be accepted in limited spheres, there is general uneasiness around it and what it might mean for the individual and society, and a general perception that more democratic involvement and control is needed. The Snowden revelations and newspaper editorials have given a strong impetus in this regard.

As a result of the public's lack of clarity about surveillance technologies, other opinion-shaping factors become significant in whether technology is accepted and the role it plays in wider debates (such as how technologies are presented in the media or the immediate reaction they elicit). Whilst the technologies and the systems in which they operate are the active features in the privacy impact, their references in relation to other debates or perceptions play an active role in public opinion formation.

Among the main points relevant to an understanding of public acceptance of surveillance are the following:

- the relationship between publics and surveillance, in terms of both technologies that are used and institutions or structures implementing and controlling surveillance;
- the relationship between surveillance and modern societies;
- the relationship between citizens, publics and modern societies;
- the risks and threats facing modern societies and citizens and responses to these.

It is difficult to draw definitive conclusions as to which theoretical framings and which elements of academic discourse present the best explanation as to the findings of surveys or the deeper reasons for these findings as a result of how citizens engage with surveillance practices and technologies. The findings of a major survey conducted by the PRISMS survey, funded by the European Commission, are expected to shed some light on this matter.[18]

Bearing these viewpoints and theoretical positions in mind is nevertheless helpful in identifying robust analytical and explanatory frameworks for examining the key issues that emerge in surveys and research exploring public acceptance of smart surveillance technologies. Understanding these theoretical framings is critical and vital in fully understanding how research is shaped by theoretical preconceptions or considerations. This allows a much more nuanced appraisal of empirical research such as the opinion surveys examined in the SAPIENT project.

6 Scenarios and stakeholder consultation workshops

As part of its work on addressing the potential impacts that current and emerging smart surveillance technologies could have on privacy and other fundamental rights, the SAPIENT consortium invited a range of different types of stakeholders to participate in scenario-based workshops. Invited participants included academics, policy-makers and representatives from industry (including private companies and R&D specialists), public authorities, law enforcement, data protection authorities (DPA), civil society organisations (CSOs) and research institutions. The consortium drafted three scenarios, focused on (1) security in public spaces, (2) border security and immigration control and (3) business practices such as personalised advertising. The goal of the scenarios was to trigger discussion among workshop participants in order to develop a view of when it is appropriate to deploy smart surveillance and how fundamental rights should be protected.

[18]The findings of the survey are expected to be published in October 2014. `http://prismsproject.eu`

Each workshop generated its own distinct discussions based on the issues raised in the scenarios. The workshops aimed to develop an understanding of over-arching issues of concern and a protection framework that can be applied to different technologies, practices and sectors. Workshop participants discussed the drivers for the use of smart surveillance technologies, the role of the current "rule of law" related to transparency and consent, the relative vulnerability of individuals and possibilities for resistance and finally, potential solutions to address threats to fundamental rights. The diversity of participants at the workshops showed how stakeholder views are spread across different categories of stakeholder, where different types of stakeholders were largely in agreement, and where conflicts need to be resolved.

6.1 Drivers for the use of smart surveillance technologies

A key issue of concern across all three workshops were the different drivers of the use of surveillance technologies that may impinge upon privacy. These included economic, social and political drivers.

Economic drivers include the ways in which private companies' interests are shaping security policies and the associated economic benefits. One of the experts from the border control workshop mentioned that many border control technologies are not designed from scratch, and were originally developed by the defence industry. These industrial companies are looking for new markets for their products, and the industry lobbies for a prevalent deployment of their technological systems at airports and other border areas. One benefit is that the creation of a market for these technologies fuels economic growth, and another is that surveillance technologies sometimes offer the possibility to design new products and services. In the personalised advertising workshop, a representative from industry argued that the potential benefits for consumers, such as the provision of free services, must be acknowledged. A representative from a consumer rights association noted the need to account for the growing market of privacy preserving tools alongside privacy intrusive techniques. However, this question of potential economic benefits, most strongly supported by industry, generated significant controversy in relation to other stakeholders.

Political drivers include the mobilisation of political issues to encourage or support the use of surveillance technologies in public space, personalised advertising contexts and border control. One participant stated that certain political circumstances would be needed to produce a situation where a police state emerges and privacy is undermined. The media often play a key role in these political mobilisations. In relation to the border control scenarios, some elements of the media have often led the debate on immigration and contributed towards the fear of huge waves of migrants stealing EU citizens' jobs and contributing to higher crime rates. On the other hand, news coverage has also contributed to a more critical public perception and sometimes even rejection of certain border control systems such as full body scanners. However, a public authority representative noted that negative headlines could also be seen as a corrective, triggering a change in the way surveillance systems are developed and deployed.

Finally, societal drivers included the need to efficiently deal with social changes. Most of the stakeholders in all three workshops, but most especially in border security, shared the opinion that, beyond privacy and data protection, there were crucial societal benefits of surveillance technologies, such as providing security, mobility and health. Policy-makers in the field of home affairs explained that the introduction of border surveillance measures were important to guarantee mobility as well as provide security and control illegal immigration which sometimes seem to be opposing tasks. A border control workshop participant referred to some human traffickers who could be arrested due to the analysis of their passenger name record data. An expert from a data protection authority argued that some important societal benefits of border control technologies could include the prevention of epidemic diseases, by being able to trace carriers of a disease back to the original source. However, each of these benefits has to be part of an approach that does not undermine privacy.

6.2 Rule of law

A second key issue to emerge from the three workshops was the ways in which current laws provide protections from the over-zealous use of surveillance technologies in all three sectors. Although some law enforcement and public authority representatives acknowledged that security providers would probably like to use technologies and data to the full extent, which would conflict with central data protection principles, all stakeholders agreed upon the importance of complying with data protection law when developing and deploying surveillance technologies. A participant with a law enforcement background reminded participants that law enforcement has to guarantee all constitutional freedoms, not just safety and security, thus data protection and other fundamental rights must also be protected by the police. Thus, surveillance operators must consider proportionality, transparency, adequacy and data ownership. However, CSO representatives in two different workshops noted that the current legal framework in Europe allows circumstances for exceptions to the protection of privacy in the public security field. Thus, CSOs felt that the rule of law was a less strong protection than public authority and law enforcement stakeholders claimed.

6.3 Transparency and consent

Participants in all three workshops identified a key failure of the current rule of law as a failure of transparency and consent. One researcher from a think tank noted in the personalised advertising workshop that the business model of some data collection and processing companies is based on the concealed processing of information. While in the border security workshop, data protection authority (DPA) representatives emphasised that, in many instances, people do not know what kind of data, e.g., biometric data, is collected by border control authorities and what happens to it (function creep). Also, the data retention period and the number of actors able to access the data, e.g., law enforcement agencies, often remain unclear. The exchange and dissemination of this data between public actors, public and private sector entities, as well as the transfer to third countries poses a threat

to an effective enforcement of data protection. Finally, purpose limitation, a central data protection principle, often cannot be guaranteed.

A representative of a civil society organisation raised the question of consent in that consumers often do not understand what happens to their data because of this lack of transparency. As a result, they do not have any effective possibility to refuse the collection and processing of their data, since the only alternative is to risk being fully excluded from a set of services. In consequence, the meaning and effectiveness of consent as a data protection measure could be lost. Nevertheless, one participant underlined the potential advantage, for both service providers and consumers, derived from a more aware involvement of customers in data collection and processing, which could ensure the delivery of a service that is more tailored to consumers' needs.

6.4 Vulnerability and resistance

In terms of those who are targeted by surveillance technologies, two key issues emerged from the workshops – the use of surveillance technologies for social sorting and the potential for citizen resistance to surveillance. Participants at the border control workshop expressed concern about social sorting at borders, and agreed that technological advances are most often accompanied by negative effects for certain groups of people, e.g., refugees and irregular migrants. Thus, border security technologies should always take the level of vulnerability of the traveller into account, as well as provide transparency over the technical processes that categorise people into desirable and non-desirable travellers. In the personalised advertising workshop, a representative from a consumer rights organisation underlined the tendency of some business models to make those who do not participate in loyalty schemes pay the costs of the benefits that they offer to clients who do participate. However, a civil liberties organisation representative pointed out that the benefits of personalised advertising primarily lie with the businesses providing the service, not the consumers. Most of the business models offering free services are requesting customers' data in exchange, and are using them to make profit. In the public space security workshop, a CSO representative pointed out that what is fundamentally different from the past is the focus on prevention by removing the potential "trouble makers" before the actual event. In this context, we are required to wonder what it takes to be regarded as a potential "trouble maker". Thus, civil society organisations were particularly concerned about citizens and consumers being vulnerable in the face of smart surveillance technologies.

Yet, individuals are not passive subjects of surveillance and may resist surveillance in unexpected ways. A participant in the public space surveillance workshop noted that citizens in Québec resisted a government law prohibiting assemblies in public spaces by organising mass strikes. In the same workshop, a representative of an R&D institution suggested that stakeholders should consider the sabotage effect, and try to understand how different actors may behave in this respect. Finally, in the border security workshop, a CSO representative noted that Frontex systems and operations may actually contribute to a higher death rate of refugees on the sea, because they take more dangerous routes in order to avoid being detected.

7 Potential solutions

In all three workshops, stakeholders proposed possible solutions to better protect privacy and other fundamental rights given the proliferation of smart surveillance technologies. For some CSO stakeholders, this meant redefining the terms of the debate. In the border security workshop, one CSO representative suggested that border security should focus on the protection of people trying to cross EU borders as well as the protection of citizens, while another argued that issues such as sustainable development co-operation and fair trade programs for developing countries should be taken more seriously when searching for an effective long-term strategy to combat illegal immigration and related security problems. However, most other stakeholders focused on possible solutions that more directly addressed the key terms of the privacy and security debate, including better enforcement of existing rules, education, privacy-by-design approaches, self-regulation and privacy impact assessments.

7.1 Better enforcement of existing rules

Even before adoption of the proposed Data Protection Regulation, workshop participants noted that significant privacy and data protection rules already exist in current legislation to provide some protections from smart surveillance technologies. However, many stakeholders felt that these rules were not enforced strongly enough, and that better enforcement would have a positive impact on citizens' privacy. This discussion was strongest in the personalised advertising workshop, where a representative of a consumer rights organisation mentioned that the EU Charter of Fundamental Rights provides significant opportunities to protect fundamental rights, but this legislation is not well enforced and individuals lack direct access courts where they could challenge practices. The idea of enhancing oversight of people was shared by a representative from a private company, who also advanced the idea of a more important involvement of the Fundamental Rights Agency, possibly along the lines of the work done by the European Data Protection Supervisor. A data protection authority representative also mentioned the role of enforcement and supervision, coupled with sanctions, to ensure respect for the chosen regulation.

Another possible solution proposed by a representative of civil society organisations was to further generalise the opt-in approach. However, private firms preferred a differentiated approach to opting in where some spheres would require a "true" opt-in, while others utilised the opt-out approach. Representatives from all stakeholder categories supported better enforcement of existing legislation. However, the following, additional suggestions demonstrate that better enforcement alone will not protect individual privacy and fundamental rights.

7.2 Education

Consumer or citizen education emerged as a second important way to improve protections for fundamental rights. This was shared between different workshops and different stake-

holder categories. In the public space workshop, a representative of a research institution argued that privacy protection depends on good communication practices with the public. Most people are not aware, and are not conscious of the concerns with respect to privacy and data protection, which is why education is crucial. In the personalised advertising workshop, a private company representative stated the ability of consumers to understand data processing schemes is crucial to ensure trust in surveillance systems. Another DPA participant underlined the role that education should play as technologies become further integrated into people's lives. Without proper education and awareness of the effective uses of personal data, data subjects will have difficulty exercising their rights, and will require higher standards of protection. One option, proposed by the same participant, was to implement a label system, as in the case of food commercialisation, which permits consumers to understand their choices between different services and systems. Finally, a participant from the CSO sector felt that it was not only consumers who needed education. Rather, law enforcement and police stakeholders also needed better education about their role in protecting privacy and personal data.

7.3 Privacy by design

Privacy-by-design approaches were mentioned in all three workshops, and primarily supported by DPA stakeholders and industry representatives involved in research and development. In the border security workshop, a DPA stakeholder recommended a privacy-by-design approach for smart surveillance technologies, such as installing a software element that automatically erases the collected data after a certain period of time. In the surveillance-in-public-spaces workshop, an R&D representative argued that because there is always a gap between the legal framework and technological progress, technology has to be included as part of the solution. Privacy enhancing technologies (PETs) and privacy-by-design principles could be implemented to assist with technological approaches to data minimisation and purpose specification. A DPA participant in the personalised advertising workshop noted that opt-in or opt-out issues were important to address in the design of an information collection system.

7.4 Self-regulation

Self-regulation was primarily discussed in the personalised advertising workshop. Representatives of private industry were particularly keen to support self-regulatory initiatives in this workshop, although one acknowledged that regulation involved three potential layers: the legislative, the administrative (DPA supervision) and the business layers. One participant proposed an alternative perspective, using a continuum of regulatory possibilities ranging from state regulation to self-regulation, and including possible forms of co-regulation as is used for RFID systems. However, a representative from a consumer rights organisation argued that self-regulation should not be used at all, because it does not work. One of the main limits of self-regulation is linked to the continuous blending of

private and public information, and the combined use of multiple technologies. Thus, different categories of stakeholder had significantly different views about the potential role of self-regulatory initiatives.

7.5 Privacy impact assessment

The co-regulatory privacy impact assessment (PIA) model was discussed in all three workshops. The proposed Data Protection Regulation contains a provision for data protection impact assessment (DPIA). One industry representative expressed concern about the ways in which PIAs are or will be carried out, their purposes and the best strategies to communicate their results once they are undertaken. According to a representative from another private firm, the experience of the United Kingdom data protection authority could be particularly useful, as the release of a public version of PIA became an integral part of the auditing routine of private companies, with a positive effect in terms of reduction of data loss. In the border security workshop, a DPA representative also offered data protection and privacy impact assessments as a tool to provide more transparency and raise awareness among producers, service providers and end users. Technologies and systems should not only fulfil the three classical principles of data security, namely confidentiality, integrity and availability, but should also meet the privacy requirements of unlinkability, transparency and intervenability. In the public space workshop, a representative from a research institution noted that impact assessments should consider risk and the acceptable level of "collateral damage" to privacy or other fundamental rights. PIAs should also consider smart surveillance systems rather than technologies, and according to a researcher from a think tank, a PIA covering different related systems should be preferred. Another PIA advocate noted a PIA model should also include other fundamental rights, for example, the freedom of communication, as well as the clear listing of all the costs engendered by a system and their distribution.

However, the use of PIA and other supervision mechanisms that rely upon stakeholder consultations engendered a discussion within the personalised advertising workshop about the issue of the asymmetrical stakeholder participation. Two different CSO participants pointed out that the availability of internal resources impacts upon an organisation's ability to participate in key meetings and key moments of decision-making. Furthermore, their lack of resources impacts upon their ability to ensure their perspective has the same weight as actors such private companies. This is particularly relevant when a co-regulation model, such as PIA, is chosen. According to a member of a civil rights group, this asymmetry in terms of weight should be compensated by the role of the government, which should not play the neutral arbiter but engage on the side of citizens. CSO representatives also noted that PIAs are often presented as "blessed" from advocacy organisations, even if their concerns or recommendations are ignored. Therefore, if civil society organisations are not able to fully and fairly engage, there is a risk that PIAs will lack credibility. Thus, civil society organisations ought to be better supported in participating in PIAs and ensuring that their concerns are given adequate consideration by governments or private companies with significantly more resources. Thus, while data protection authorities, think tank representatives and

some industry representatives welcome the introduction of measures such as PIAs, other stakeholders point out considerable issues in their implementation.

8 Developing a surveillance impact assessment

A principal goal of the SAPIENT project was to develop and test a surveillance impact assessment. To that end, the consortium first examined the state of the art in privacy impact assessment to see what lessons or best practices could be applicable to an SIA methodology.

8.1 Drawing on the state of the art in privacy impact assessment

A PIA can been defined as

> "a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts. A PIA is more than a tool: it is a process that should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until and even after the project has been deployed."[19]

The SAPIENT consortium reviewed existing privacy impact assessment methodologies, notably those used in Australia, Canada, France, Ireland, the Netherlands, New Zealand, the US, UK[20] and what is foreseen at the EU level, to determine their suitability as a means (1) to verify that surveillance systems and the sharing of information is respecting the privacy of the citizens, (2) to limit the collection and storage of unnecessary data and (3) to find a balance between data collections needs and data protection and privacy. The consortium also analysed examples of PIAs targeted to surveillance technologies and applications.

The consortium identified certain key features and limits of each of the existing PIA methodologies.[21] Indeed, each of the PIA methodologies has some interesting features that could be included in a PIA suitable for development and deployment of smart surveillance technologies and systems. On the other hand, it was also important to understand the limits of

[19] Wright, David, "The state of the art in privacy impact assessment", Computer Law & Security Review, Vol. 28, No. 1, 2012, pp. 54-61.

[20] This selection is not limited to countries where the methodologies are formally labelled PIA: it also encompasses other PIA-like methodologies. This selection is linked to the need to understand the development and deployment of PIA-like measures within different institutional cultures.

[21] For example, the UK emphasises early consultation with stakeholders, including the public. Canada emphasises the need for government departments and agencies to submit a proper PIA with their funding submissions to the Treasury Board. In addition, PIAs must be forwarded to the Office of the Privacy Commissioner of Canada, who can and does audit PIAs. Canada publishes summaries of PIAs on departmental websites. US government agencies, such as the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB), are supposed to publish full PIAs on their websites (redacted as necessary).

already existing PIA methodologies, and to check them against the features and the challenges of present and prospective smart surveillance technologies and practices.

The review of the state of the art in PIA served as an important foundation for the development of a surveillance impact assessment methodology. Nevertheless, surveillance systems and technologies have particularities that go beyond PIAs. In many cases (e.g., in law enforcement applications), surveillance has security sensitivities not typically found in other issues involving data protection; second, existing PIA methodologies are especially focused on data protection, and less focused (or not at all) on the wider privacy issues related to privacy of communications (e.g., intercepts), privacy of the body (body searches), privacy of behaviour (video surveillance). In additional, surveillance may interfere with other fundamental human rights and ethical values, which should be taken into consideration while analysing the impacts of these technologies or practices.

The consortium extracted the best elements and identified the main limits of existing PIAs and categorised a set of recommendations for a surveillance impact assessment (SIA) methodology for the EU. To our knowledge, the consortium's study was the first to make a comparative analysis of different PIA methodologies with a view to extracting the elements that can be used in constructing a surveillance impact assessment methodology. The consortium's findings can be used by policy-makers and industry decision-makers to "flesh out" the rather sketchy provisions for a data protection impact assessment (which is a more circumscribed version of a PIA) in Article 33 of the proposed Data Protection Regulation.

In Article 33 of the proposed Data Protection Regulation, the European Commission made data protection impact assessment (DPIA) mandatory "Where processing operations present specific risks to the rights and freedoms of data subjects". While Article 33 has much to commend it, its emphasis seems to be more on the DPIA report rather than on the PIA process. The Art. 29 Working Party has suggested some helpful improvements to Article 33. In addition to those, the EC (and an SIA handbook) could usefully highlight the benefits of a PIA and/or SIA.

A key issue has been the adequacy of a PIA to address the range of issues raised by the deployment of surveillance technologies and systems. In sum, the consortium concluded that constructing an SIA was necessary because surveillance systems and technologies raise more than just privacy issues.

8.2 An SIA is more than a PIA

A paper co-authored by Wright and Raab (2012)[22] became, in effect, the first draft of the SIA methodology. Nevertheless, the SAPIENT partners had numerous conference calls, exchanges of e-mails and face-to-face meetings to further develop and refine the methodology, which underlined the challenges of producing an SIA methodology. The draft SIA went through more than 20 iterations. One of the key differences between a PIA and an SIA is that the latter needs to consider not only the impacts on privacy of surveillance systems and

[22] Wright, David and Charles Raab, "Constructing a surveillance impact assessment", Computer Law & Security Review, Vol. 28, 2012, pp. 613-626.

technologies, but also the societal, economic, political, legal and ethical impacts, because surveillance raises other issues in addition to privacy. Furthermore, because surveillance does raise other issues, a wider range of stakeholders should be engaged in the process. Hence, the consortium's 41-page SIA guide essentially described a method for identifying, assessing (or evaluating) and prioritising for treatment risks arising from the development and deployment of surveillance technologies, systems and applications. The SIA guide was divided into two main parts and three annexes. The first part provided an overview of a risk assessment approach to SIA. The second part concerned the conduct of an SIA. Annex A provided a set of criteria and questions related to the aforementioned impacts. Annex B provide examples of assets, threats, vulnerabilities and consequences involved in surveillance. Annex C provided a template for assigning values to those assets, threats, vulnerabilities and consequences.

The guide states that the purpose of a surveillance impact assessment is to assess the risks that a surveillance system, technology, service or other initiative poses for privacy, as well as for other human rights and ethical values. The risk assessment addresses the likelihood of a certain event and its consequences, i.e., impacts. An SIA should include stakeholder consultation and, ultimately, lead to remedial actions as necessary in order to avoid, minimise, transfer or share the risks. The SIA should follow a surveillance initiative throughout its life cycle. The project should revisit the SIA as it undergoes changes or as new risks arise and become apparent.

While privacy and data protection impacts are a major focus of an SIA, surveillance affects a range of other fundamental rights and ethical and social principles that may also be relevant in a particular assessment.

A surveillance impact assessment may be undertaken (1) by those developing surveillance systems or technologies or (2) by those who are commissioning (procuring) and intending to operate a surveillance system or (3) by regulators who want to assess surveillance system proposals.

Three main principles should govern the development and deployment of surveillance systems:

1. Surveillance systems should comply with the law.
2. Surveillance should be used only when there are no more cost-effective alternatives.[23]
3. Surveillance systems should be ethically defensible.

To ensure these principles, three main tasks should be undertaken before and/or during development and deployment of a surveillance system:

- The proposed surveillance system should undergo an SIA before or concurrently with development of the technology or system.

[23] Cost here should be understood in a wider sense than just monetary cost, for example, social costs, opportunity costs, political costs, etc.

- Mass surveillance systems should be subject to regulatory approval before deployment – i.e., an appropriate regulator would need to approve a surveillance system before it is deployed.
- The SIA and the surveillance system should be subject to an audit.

An assessment of the risks or impacts of a prospective surveillance system should

- identify the risk criteria – the framework within which risks will be assessed
- identify the risks, which is the process of enumerating feared events from stakeholders and the corresponding threats that might lead to them.
- analyse the risks, which is the process of understanding the nature of the risk and determining the consequences and likelihood of each risk
- assess (evaluate) the risks, which is the process of ranking or prioritising the risks: which risks are the most serious and should be dealt with first.

The organisation that "owns" (or is responsible for) the risk should carry out the risk treatment and identify controls or counter-measures to avert the risks.

The assessor should identify, analyse and evaluate the threats and vulnerabilities to individuals and groups (including society), assess the impacts (consequences) of the risk involved, and recommend measures and controls to manage them.

Having identified relevant risks, the organisation should identify how it intends to treat those risks, i.e., which controls (or counter-measures) will mitigate those risks? The risk treatment may involve reducing, eliminating, transferring or insuring against those risks.

A surveillance impact assessment (SIA) should be regarded as a *process*, comprising the following main steps.[24] The SIA *report* documents the process.

The specific steps followed and the attention (and resources) devoted to each step will be a matter of judgement and how credible the organisation responsible for the impact assessment wishes the report to be.[25] A high-level overview is given below, and illustrated in Figure 1.

The list of the key steps for the SIA follows:[26]

[24] This surveillance impact assessment guidance draws on ISO 27005, ISO 31000, CNIL's privacy risk methodology, ENISA's risk management guidance, NIST 800-30 and EBIOS and on Wright, David, and Kush Wadhwa, "A step-by-step guide to privacy impact assessment", Paper presented at: Second PIAF workshop, 24 April 2012, Sopot, Poland, 2012. `http://www.piafproject.eu/Events.html`

[25] Two examples, one from the private sector and one from the public sector, of well-conducted and credible privacy impact assessments are the following: Engage Consulting Limited, "Privacy Impact Assessment: Use of Smart Metering data by Network Operators", ENA-CF002-007-1.0, Energy Networks Association, London, 2011; Department of Energy and Climate Change (DECC), "Smart Metering Implementation Programme – Privacy Impact Assessment", London, 2012.

[26] For a more comprehensive description of the assessment process, see Wright, David and Michael Friedewald, "Integrating privacy and ethical impact assessment", Science and Public Policy, Vol. 40, No. 6, 2013, pp. 755-766; Wright, David, Kush Wadhwa, Monica Lagazio, et al., "Integrating privacy impact assessment in risk management", International Data Privacy Law, Vol. 4, No. 2, 2014, pp. 155-170; Wright, David, "Making Privacy Impact Assessment More Effective", The Information Society, Vol. 29, No. 5, 2013, pp. 307-315.

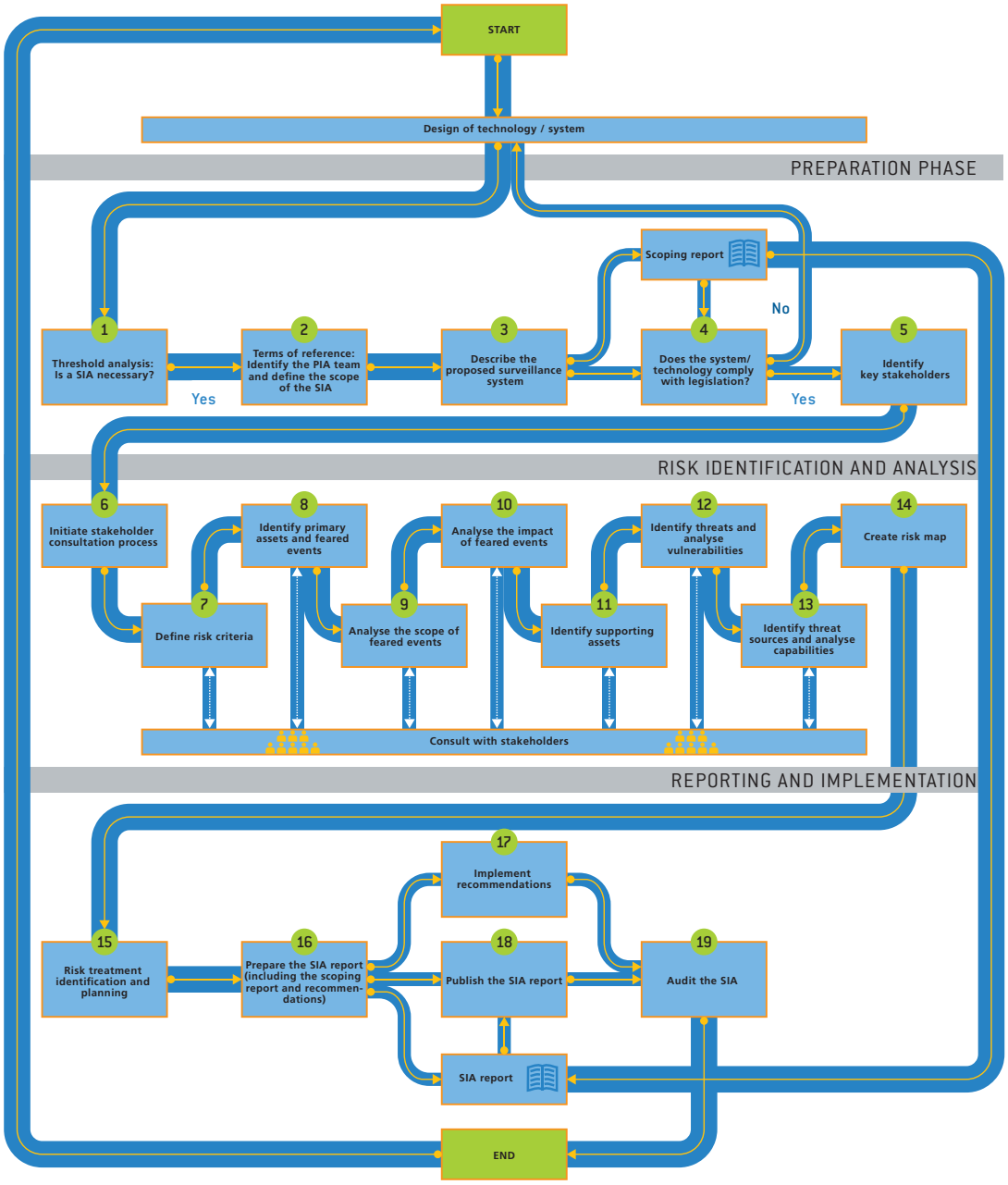

Figure 1: Impact Assessment Process

Phase I: Preparation

- Determine if a SIA is necessary.
- Develop terms of reference for surveillance assessment team.
- Prepare a scoping report (What is the scope of the surveillance system?).
- Check compliance with legislation.
- Identify key stakeholders.

Phase II: Risk identification and analysis

- Initiate stakeholder consultation.
- Identify risk criteria.
- Identify primary assets and feared events (what could happen if the surveillance system is implemented?).
- Analyse the scope of feared events.
- Analyse the impact of feared events.
- Identify supporting assets.
- Identify threats and analyse vulnerabilities.
- Identify threat sources and analyse capabilities.
- Create a risk map (for prioritising risks for treatment).

Phase III: Risk treatment and recommendations

- Risk treatment identification and planning
- Prepare an SIA report.
- Record the implementation of the report's recommendations.
- Publish the SIA report.
- Audit the SIA.
- If necessary, update the SIA.

These various steps are not fixed in concrete. They may vary depending on the scale and scope of the surveillance system and the sequence in which they are undertaken.

An important part of an SIA is engaging stakeholders. There are many reasons for doing so, not least of which is that they may identify some privacy or ethical or societal risks not considered by the project manager or assessor. By consulting stakeholders, the project manager may forestall or avoid criticism that they were not consulted. If something does go wrong downstream – when the surveillance system or technology is deployed – an adequate consultation at an early stage may help the organisation avoid or minimise criticism and perhaps liability. Furthermore, consulting stakeholders may provide a sort of "beta test" of

the system or technology. Consulted stakeholders are less likely to criticise a project than those who were not consulted.

Having finally agreed the SIA methodology, the SAPIENT consortium sent out an invitation letter to 140 companies inviting them to take part in an SIA case study free of charge. In total, three replies were received, which culminated in a number of changes being made to the full methodology.

The consortium developed and streamlined the SIA as a result of feedback from the companies contacted. As noted above, the full SIA methodology consisted of a 41-page document. The revised SIA was developed into a 10-page document. Both of the approaches are found to have value, again depending on the scale and scope of the surveillance system being considered.

8.3 Lessons learned from the case studies

The main lessons drawn from the SIA case studies were:

- To keep the process simple
- Participants may be hesitant to undertake the risk-mapping exercise
- The importance of external stakeholders
- The importance of getting detailed information on the project in terms of information flows
- One size does not fit all.

The importance of keeping the process simple cannot be over-emphasised. It can make a real difference in relation to whether an organisation will choose to pursue an SIA, and ensures that the time spent conducting the SIA is clearly structured and not overly complex. The outcome of the SIA case studies also showed that the risk-mapping element of the methodology could be revisited and revised in order to make the process less formalistic. Most people with whom the consortium conducted the SIAs prefer an open discussion on risks and possible solutions, rather than a structured hypothesising of the likelihood and severity of risks.

Contacting stakeholders and receiving feedback showed how important it is to have the input of interested, and knowledgeable, but independent parties, into the SIA process. This provides a greater variety of perspectives (ethical, social, legal, etc.). After having spoken to a number of stakeholders, the SAPIENT team are of the view that it is imperative to get the feedback of external stakeholders, even if it is just a brief response via e-mail. Preferably, external stakeholder engagement could take the form of a carefully planned focus group or workshop, or, if that is not possible, then in-depth phone discussion on a one-to-one basis.

Obtaining a detailed description of the project is imperative for the conduct of an SIA. A clear understanding of the information flows must be obtained prior to embarking on any discussion on risks and possible solutions. Finally, the outcome of the case studies suggests strongly that one size does not fit all in relation to surveillance impact assessments. The

SIA questionnaire should be moulded to the specificities and needs of each organisation, rather than one set of questions being applicable to every situation and system and/or technology.

Furthermore, conducting an SIA may involve undertaking the risk assessment element in a less formulaic manner than that which is described in the revised version of the SIA. However, these elements can be included depending on the context, rather than attempting to develop a guide to suit every situation, organisation and context.

9 Conclusions

The SAPIENT consortium's experience in developing a "full" SIA methodology as well as a streamlined version mirrors somewhat the experience of the UK Information Commissioner's Office (ICO). The ICO developed an 84-page PIA guide, which was subject to various criticisms from stakeholders, chief among which was that the PIA guide was too long and complicated. As it turned out, Trilateral, one of the SAPIENT partners, conducted a study for the ICO on PIA and risk management in the first half of 2013.[27] As part of that study, Trilateral conducted a survey of 829 central government departments, companies, National Health Service (NHS) trusts and local authorities. Virtually all respondents to the Trilateral survey said the ICO PIA guide should be streamlined and made more user friendly. Following the Trilateral report, the ICO did, in fact, produce a more streamlined, principles-based PIA guide.

While the streamlined SIA developed for the SAPIENT project might be suitable for relatively small surveillance projects, the consortium continues to believe that bigger, more complicated surveillance projects require a much more detailed assessment, not only of the surveillance system's impacts on all seven types of privacy[28], but also of the ethical, legal, social, economic and political impacts. The SAPIENT project has developed (as far as it knows) the world's first such methodology. Not only has SAPIENT developed the process for conducting the SIA, it also developed a set of questions aimed at uncovering the privacy, ethical and other impacts, which should help anyone – regulators, companies, consultants – conducting an SIA.

The consortium also believes that the conduct an SIA – one engaging stakeholders – should help avoid some of the worst risks arising from surveillance.

References

[1] Albrechtslund, Anders, "Ethics and technology design", Ethics and Information Technology, Vol. 9, 2007, pp. 63-72.

[27] For a description of the ICO study and a review of its results, see Wright, et al., 2014.

[28] Finn, Rachel L., David Wright and Michael Friedewald, "Seven types of privacy", in Gutwirth, Serge, et al. (eds.), European Data Protection: Coming of Age, Springer, Dordrecht, 2013.

[2] BVerfGE 115; 320, "Rasterfahndung II", 4 April 2006. http://http://www.bundesverfassungsgericht.de/entscheidungen/rs20060404_1bvr051802.html.

[3] Cameron, Iain, "Report to the Swedish Foreign Office on Targeted sanctions and legal safeguards", 2002. http://resources.jur.uu.se/repository/5/PDF/staff/sanctions.pdf

[4] Cortright, David, and George A. López (eds.), Smart sanctions: targeting economic statecraft, Rowman & Littlefield, New York, 2002.

[5] De Hert, Paul, and Vagelis Papakonstantinou, "The Police and Criminal Justice Data Protection Directive: Comment and Analysis", Computers & Law Magazine of SCL, Vol. 22, No. 6, 2012, pp. 21 - 25.

[6] Department of Energy and Climate Change (DECC), "Smart Metering Implementation Programme – Privacy Impact Assessment", London, 2012.

[7] Engage Consulting Limited, "Privacy Impact Assessment: Use of Smart Metering data by Network Operators", ENA-CF002-007-1.0, Energy Networks Association, London, 2011.

[8] European Commission, "A comprehensive approach on personal data protection in the European Union", COM(2010) 609 final, Brussels, 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF

[9] European Commission, "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offencesor the execution of criminal penalties, and the free movement of such data", COM(2012) 10 final, Brussels, 2012. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0010&from=en

[10] European Commission, "Impact Assessment Accompanying the General Data Protection Regulation", SEC(2012) 72 final, European Commission, Brussels, 2012. http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012SC0072

[11] European Union Agency for Fundamental Rights, "Opinion on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final)", FRA Opinion 1/2011, Vienna, 2011. http://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_EN.pdf

[12] Finn, Rachel L., David Wright, and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert, and Yves Poullet (eds.), European Data Protection: Coming of Age, Springer, Dordrecht, 2013, pp. 3-32.

[13] Goold, Benjamin J., "Surveillance and the Political Value of Privacy", Amsterdam Law Forum, Vol. 1, No. 4, 2009, pp. 3-6. http://www.amsterdamlawforum.org/

[14] Gutwirth, Serge, Rocco Bellanova, Michael Friedewald, Dara Hallinan, David Wright, Paul McCarthy, Julien Jeandesboz, Emilio Mordini, Silvia Venier, Marc Langheinrich, and Vlad Coroama, "Smart Surveillance - State of the Art Report", Deliverable 1.1, SAPIENT Project, 2012. http://www.sapientproject.eu/docs/D1.1-State-of-the-Art-submitted-21-January-2012.pdf

[15] Kranzberg, Melvin, "Technology and History: "Kranzberg's Laws"", Bulletin of Science, Technology and Society, Vol. 15, No. 1, 1995, pp. 5-13.

[16] Kreissl, Reinhard, Clive Norris, Marija Krlic, Leroy Groves, and Anthony Amicelle, "Surveillance: preventing and detecting crime and terrorism", in David Wright, and Reinhard Kreissl (eds.), Surveillance in Europe, Routledge, London, New York, 2015, Forthcoming.

[17] Maras, Marie-Helen, "The economic costs and consequences of mass communications data retention: is the data retention directive a proportionate measure?", European Journal of Law and Economics, Vol. 33, No. 2, 2011, pp. 447-472.

[18] Wright, David, Michael Friedewald, Serge Gutwirth, Marc Langheinrich, Emilio Mordini, Didier Bigo, Rocco Bellanova, Kush Wadhwa, and Sergio Carrera, "Sorting out smart surveillance", Computer Law & Security Review, Vol. 26, No. 4, 2010, pp. 343-354.

[19] Wright, David, "The state of the art in privacy impact assessment", Computer Law & Security Review, Vol. 28, No. 1, 2012, pp. 54-61.

[20] Wright, David, and Charles Raab, "Constructing a surveillance impact assessment", Computer Law & Security Review, Vol. 28, 2012, pp. 613-626.

[21] Wright, David, and Kush Wadhwa, "A step-by-step guide to privacy impact assessment", Paper presented at: Second PIAF workshop, 24 April 2012, Sopot, Poland, 2012. http://www.piafproject.eu/Events.html

[22] Wright, David, "Making Privacy Impact Assessment More Effective", The Information Society, Vol. 29, No. 5, 2013, pp. 307-315.

[23] Wright, David, and Michael Friedewald, "Integrating privacy and ethical impact assessment", Science and Public Policy, Vol. 40, No. 6, 2013, pp. 755-766.

[24] Wright, David, and Charles Raab, "Privacy principles, risks and harms", International Review of Law, Computers & Technology, Vol. 28, No. 3, 2014.

[25] Wright, David, Kush Wadhwa, Monica Lagazio, Charles Raab, and Eric Charikane, "Integrating privacy impact assessment in risk management", International Data Privacy Law, Vol. 4, No. 2, 2014, pp. 155-170.

Co-ordinator:
Dr. Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Straße 48 | 76139 Karlsruhe | Germany
Phone: +49 721 6809-146 | Fax +49 721 6809-315
michael.friedewald@isi.fraunhofer.de