Developing and testing a surveillance impact assessment methodology

David Wright*, Michael Friedewald**, and Raphaël Gellert***

Abstract

- With the increasing pervasiveness of surveillance, from big companies such as Google and Facebook, as well as from the intelligence agencies, such as the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ), there is a clear need for a surveillance impact assessment (SIA), a method that addresses not only issues of privacy and data protection, but also ethical, social, economic, and political issues.
- The SAPIENT project, funded by the European Commission, and undertaken by a consortium of partners from several European countries, aimed to develop an SIA methodology, based on stakeholder needs and a set of scenarios.
- This paper describes how the SAPIENT consortium developed its SIA methodology and some of the key elements comprising the methodology.
- The consortium tested the SIA in several cases studies. So far as the consortium knows and is concerned, this was the first time that an SIA methodology was developed and tested in real case studies—the results of which led to development of a streamlined version of the SIA.

Introduction

More and more business—not only Facebook and Google—are surveilling users while security agencies argue that more data means more effective law enforcement. With the increasing pervasiveness of mass surveillance, there is a clear need for a surveillance impact assessment (SIA), a method that addresses not only issues of privacy and data protection, but also ethical, social, economic, and political issues. This paper describes the development and testing of an SIA, which was developed in the SAPIENT project, which was funded by the European Commission, and undertaken by a consortium of European partners.

The specific 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 and at informing the development of an SIA.

The consortium adapted a privacy impact assessment (PIA) 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 (ie an SIA methodology), which it tested on four different surveillance projects. 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.

The first step towards development of the SIA was a state-of-the-art review of surveillance technologies.

* Trilateral Research, London W14 8TH, UK. Email: david.wright@trilateralresearch.com.

** Competence Center Emerging Technologies, Fraunhofer-Institut für System- und Innovationsforschung ISI, Breslauer Straße 48, 76139 Karlsruhe, Germany.

*** Research Group on Law Science Technology & Society (LSTS), Vrije Universiteit Brussel (VUB), Pleinlaan 2, 1050 Brussels, Belgium.

The authors acknowledge the contributions to the original research on which this article is based made by Inga Kroener, Monica Lagazio, Rachel Finn (Trilateral); Dara Hallinan (Fraunhofer); Rocco Bellanova, Serge Gutwirth, Matthias Vermeulen (VUB-LSTS); Marc Langheinrich (University Lugano). The authors also acknowledge the funding provided by the European Commission to the SAPIENT project under grant number 261698 of the Seventh Framework Programme. SAPIENT is the acronym for Supporting fundamentAl rights, PrIvacy and Ethics in surveillance Technologies. The views expressed in this article are those of the authors alone and are in no way intended to reflect those of the European Commission or anyone else.

To this end, the consortium developed a taxonomy of surveillance technologies and applications, their functions, stakeholders and drivers, and purposes. From this base, the consortium examined the increasing linkages or interconnections or assemblages between different types of surveillance technologies, which is the subject of the following section.[1]

The challenges of smart surveillance technologies

Current and emerging technologies are increasingly being organised into assemblages or 'smart surveillance' systems, where surveillance systems are becoming integrated, multi-modal, 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 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] Emerging forms of surveillance are becoming pervasive in our daily lives and the public appears to have accepted some, but not all 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.

But it is not just that surveillance systems are becoming pervasive. They are also 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 prohibited 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 has been a particular goal of many surveillance-related research initiatives of both the EU Seventh Framework Programme and the US Defense Advanced Research Projects Agency (DARPA).[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, remotely piloted 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]

One way of resisting the unbridled proliferation of mass surveillance systems is to ensure our legal system is robust enough, that it has the necessary safeguards against abuses of our fundamental rights.

1 Michael Friedewald and others, *Smart Surveillance - State of the Art Report*, SAPIENT Project (2012).

2 David Wright and others, 'Sorting Out Smart Surveillance' (2010) 26 Computer Law & Security Review 343.

3 Friedewald, n 1 above.

4 BJ Goold, 'Surveillance and the Political Value of Privacy' (2009) 1 Amsterdam Law Forum 3.

Some legal issues pertaining to smart surveillance

The SAPIENT consortium analysed some of the legal issues that come to the fore in the context of smart surveillance. At times, they concern the fundamental rights impacted by these practices; at others, they deal with the application intricacies of specific legal provisions. Overall, they aim at proposing a reflection on how to enhance the legal mechanisms that apply in cases of smart surveillance. Several elements—or points of reflection—are proposed as a first step.

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, ie 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. In the context of biometric passports, the Court of Justice of the European Union (CJEU) has insisted on the dangers of centralising the storage of biometric data as it creates risks of re-use and repurposing of data, thereby directly contradicting the proportionality and data minimisation principles.[5] 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 European Commission's support for the principle of data minimisation, as reflected in the proposed Data Protection Regulation.[6] Support for the principle has also emanated from other EU bodies, amongst which the CJEU may be the most important. In a recent case, the CJEU declared the Data Retention Directive invalid partly because of its blanket requirement to preventively retain personal data without distinguishing between types of data or the purposes of the retention.[7] In the context of electronic communications, the CJEU has also warned against general obligations on the monitoring of electronic communications.[8]

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.[9] 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.[10]

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. For instance, 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 do not trigger the pre-defined alerts

5 C-291/12—Schwarz, §§ 58–59.

6 The support for this principle is even more explicit in the proposal adopted by the European Parliament, since the name of the principle (ie, 'data minimisation') is explicitly included in the text of Art. 5.3.

7 See *Joined cases C-293/12 and C-594/12—Digital Rights Ireland, Seitlinger and Others*, in particular § 46. On the link between the data quality principles and the proportionality and necessity test, see, for instance, Art. 29 WP, Opinion 03/2013 on purpose limitation, part II; Art. 29 WP, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector. In this last opinion, the Working Group makes a clear link between the data quality principles of Directive 95/46/EC and the data minimisation principle, which is, according to the latter a combination of 6.1(b) and (c). For a similar interpretation, see R Gellert and others, 'A Comparative Analysis of Anti-Discrimination and Data Protection Legislations', Chapter 4, in B Custers and others (eds), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases* (Springer 2013) 61; Serge Gutwirth, *Privacy and the Information Age* (Rowman & Littlefield 2002) 158. Such clarifications remain useful even though the principle has now been enshrined into the proposed Regulation.

8 *C-70/10—Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*; Court of Justice of the European Union (CJEU): *C-461/10–Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB.*

9 See, for instance, David Cortright and George A López (eds), *Smart Sanctions: Targeting Economic Statecraft* (Rowman & Littlefield 2002).

10 Iain Cameron, 'Report to the Swedish Foreign Office on Targeted sanctions and legal safeguards' (2002).

of these smart surveillance systems would not be affected by their use, which, consequently, does not amount to an interference with their rights. This can be seen as a response to previous criticism addressed at 'dumb forms of surveillance'. It has been argued, for instance, that these forms of surveillance relying upon the blanket collection of personal data create so-called shadows of suspicion, and stigmatisation.[11] Such criticism has been spurred both by the European Court of Human Rights (ECtHR) (in *Marper*) and by the CJEU (*Huber*).[12]

Smartness in this sense should be understood as a way to avoid the indiscriminate and disproportionate processing of personal data. Two elements should nevertheless be highlighted. A first caveat could be framed as the 'productive effect of data protection' on the legal and policy framework surrounding these technologies: these institutional responses have been brought within the legal setting offered by data protection legislation and have thus manoeuvred within the constraints of the latter. This has at times produced paradoxical effects. This is clear in the case of body scanners—renamed security scanners in the meantime—which have started processing anonymised body images, that is, eventually non-personal data, so that ultimately they would be out of reach of the data protection legislation.[13]

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 information only gathered and not always subsequently used in practice is irrelevant for the application of Article 8 of the European Convention on Human Rights (ECHR).[14] Therefore, it represents in itself a form of intrusion in private life, which should be assessed according to the test established in Art. 8(2) ECHR. Furthermore, it should be clear that the mere retention and/or collection of data already constitutes a processing as such in the meaning of Art. 2(b) of Directive 95/46/EC on the processing of personal data.[15]

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, not an operator. 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 with humans, is, by default, less discriminatory, and therefore their use should be further extended in order to compensate for human prejudices. In this sense, smartness can be associated with greater predictability and control—themselves descending from greater data granularity, as is the case in the smart meters debate.[16]

This does not mean, however, that no discrimination concerns arise. The idea that machines by definition enforce 'neutral' criteria is misleading.[17] This is why an important part of the computer science literature has been working towards so-called discrimination aware data mining, which tries to infuse discrimination sensitivity within computer technology, and which emphasises that the latter can be at most a support in decision-making processes, but can never produce discrimination-free decisions (hence the need for human intervention into the process).[18]

11 Which are clearly linked to issues of discrimination and right to a fair trial. For an analysis in this sense, see SAPIENT D3.1, pp. 39–41.

12 ECJ, *Huber*, C-524/06, 2008. 145 S. and *Marper v. The United Kingdom*, Applications nos. 30562/04 and 0566/04, European Court of Human Rights, Judgment of 4 December 2008, § 122. For an analysis of the two cases in relation to these so-called shadows of suspicion, see Gloria González Fuster and others, 'Huber, Marper and Others: Throwing New Light on the Shadows of Suspicion', INEX Policy Brief, No. 11, Centre for European Policy Studies (CEPS 2010) 4.

13 See Rocco Bellanova and Gloria González Fuster, 'Politics of Disappearance: Scanners and (Unobserved) Bodies as Mediators of Security Practices' (2013) 7 International Political Sociology 188.

14 'The storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Art. 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.

15 Processing of personal data means: 'any operation or set of operations which is performed upon personal data (. . .) such as collection (. . .).' See also the case law quoted *supra* on the retention of personal data in the electronic communication sector, where such retention is clearly envisaged by the CJEU as a processing in the meaning of Art. 2(b).

16 For a recollection of the pros and cons of greater granularity in smart meters, see C Cuijpers and B Koops, 'Smart Metering and Privacy in Europe: Lessons from the Dutch Case' in S. Gutwirth and others (eds), *European Data Protection: Coming of Age (?)* (Springer 2013) 269.

17 Melvin Kranzberg, 'Technology and History: "Kranzberg's Laws"' (1995) 15 Bulletin of Science, Technology and Society 5–13; Albrechtslund, Anders, 'Ethics and Technology Design' (2007) 9 Ethics and Information Technology 63–72. See also L. Winner, 'Do Artifacts Have Politics?' (1980) 109 Daedalus 121.

18 See Dino Pedreschi, S Ruggieri and F Turini, 'Discrimination-aware Data Mining', *Proceedings of KDD'08*, (2008) ACM 560; Bettina Berendt and Preibusch Sören, 'Better decision support through exploratory discrimination-aware data mining: foundations and empirical evidence' (June 2014) 22 (2) *Artificial Intelligence and Law* 175. For a seminal article on the legal issues associated with profiling and data mining, see Tal Zarsky, '"Mine your own business!": Making the case for the implication of the data mining of personal information in the forum of public opinion' (2003) 5 (1) *Yale Journal of Law and Technology* 1.

The protection afforded by Art. 15 of the Data Protection Directive (as well as Art. 4 of the proposed Regulation) against automated individual decisions should therefore be understood in the light of the above paragraph.[19] A similar protection is envisaged in Recital 20 and Article 3(5) of the European Commission's Passenger Name Record (PNR) proposal which provides 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 PNR data.[20]

Concretely, in the case of body scanners and smart CCTV cameras, no decision with a negative effect should be taken without further verification by an operator. Smart surveillance technologies only help the operator to focus his attention on persons who—according to the machine—appear to be of interest.

To some extent, these issues are the counterpoint to the ones highlighted in the previous paragraph. The threat here is not the indiscriminate collection and processing of data, but on the contrary such explicitly discriminatory practices. In the light of the risks posed by prior machine profiling, safeguards are definitely warranted, 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[21] could become an important step to ensure oversight on the entire surveillance process.

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 12 March 2014) is a welcome development in the provision of the EU with a consistent data protection framework.[22] Such a framework would in particular be helpful for solving the seemingly inextricable legal PNR-knot, but it is relevant for other smart surveillance techniques as well. One of the reasons why the CJEU dismissed the PNR agreement in 2006 was the lack of a legal basis, since Art. 95 of the Treaty establishing the European Community (TEC) and the Data Protection Directive were not suitable bases.[23]

Not all operators of smart CCTV cameras or body scanners resort under the law enforcement sector in certain Member States: one of the findings of the SAPIENT project concerned the increasingly blurry distinction between processes for the private and law enforcement sector.[24] The comprehensive framework set out in the European Commission'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.[25] 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.[26,27] 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.[28] Furthermore, the latter does not explicitly mention the data minimisation principle.

19 Art. 15 grants individuals the right not to be subject to a decision that produces legal effects concerning them or significantly affects them and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to them.

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

21 <https://fra.europa.eu/en/opinion/2011/fra-opinion-proposal-passenger-name-record-pnr-directive>.

22 As of September 2014, the European Council had not yet reached an agreement on the proposed Regulation.

23 Joined Cases C-317/04 and C-318/04 (judgment of 30 May 2006/*European Parliament v Council of the European Union*).

24 Such blurring is particularly evident in the case law of the CJEU, which confirmed that the retention and monitoring of communication data could be enacted both for law enforcement purposes and in the framework of civil litigation by electronic communication services and/or network providers, Case C-275/06 (Judgment of 29 January 2008)/Reference for a preliminary ruling from the Juzgado de lo Mercantil No 5 de Madrid—Spain/*Productores de Música de España (Promusicae) v Telefónica de España SAU*. Furthermore, Art. 13 of the data protection Directive provides an explicit nexus for the processing of data for law enforcement purposes.

25 See Art. 29 WP, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector.

26 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 offences or the execution of criminal penalties, and the free movement of such data {SEC(2012) 72 final} {SEC(2012) 73 final}.

27 See also Paul De Hert and Vagelis Papakonstantinou, 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis' (2012) 22 Computers & Law Magazine of the SCL 21, published by the Society for Computers and Law.

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

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'.[29]

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'. Personal data protection understood in this sense, however, may have the counter-productive effect of marginalising the concept of personal data and the whole legislative framework that descends from it. We evidenced this situation *supra*, with the example of security scanners.

Has privacy been left behind?

Most of the legislative attention at the European level is devoted to improving the rules and legislation regarding data protection.[30] 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 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. As a mirror to the issue highlighted in the previous section on the relevance of the notion of personal data as a legal category underpinning the whole rationale of a legal framework devised to protect citizens' fundamental rights, the right to privacy points towards possible solutions. The ECtHR has long made clear that the notion of personal data and private life are distinct, and that there can be processing of non-personal data that will infringe the right to privacy and *vice versa*.[31]

In addition, the protection regime of privacy is distinct from that of data protection, although the CJEU has had a tendency to conflate both, especially in its earlier data protection case-law,[32] but not only.[33]

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. 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 far future.[34]

The rule of law is not the only factor determining the acceptability (or not) of mass surveillance systems. Public opinion also has a role to play, as the next section indicates.

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

30 David Wright and Charles Raab, 'Privacy Principles, Risks and Harms' (2014) 28 International Review of Law, Computers & Technology 3. DOI: 10.1080/13600869.2014.913874. <http://www.tandfonline.com/doi/full/10.1080/13600869.2014.913874>.

31 *Amann v Switzerland* of 16 February 2000, § 65, *Rotaru v Romania* of 4 May 2000, § 43; *P.G. & J.H. v U.K.*, of 25 September 2001, § 57. See also P De Hert and S Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action', in S Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2002) 3; Raphaël Gellert and Gutwirth Serge, 'Beyond accountability, the Return to Privacy?', in Daniel Guagnin and others. *Managing Privacy through Accountability* (Palgrave Macmillan 2012) 261.

32 Joined Cases C-465/00, C-138/01, and C-139/01 (Judgment of 20 May 2003)/Reference for a preliminary ruling from the Verfassungsgerichtshof and Oberster Gerichtshof: *Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others* and between Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01), and Österreichischer Rundfunk; see also Gloria González Fuster and Raphael Gellert, 'The Fundamental Right of Data Protection in the European Union: in Search of an Uncharted Right', (2012) 26 International Review of Law, Computers & Technology 73.

33 See a more recent case Joined Cases C468/10 and C469/10—sociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C468/10), Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C469/10) v Administración del Estado.

34 For a similar critical appraisal of data protection, see Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement: Opacity of the Individuals and Transparency of Power', in E Claes, A Duff and S Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006) 61; however, see *contra* the Art. 29 WP, Opinion 03/2013 on purpose limitation, wherein the Working Party explicitly locates the genealogy of the purpose specification principle within the proportionality test contained in Art. 8.2 ECHR.

Public opinion should be factored into SIAs

Beyond technology and the operators of surveillance systems, the scope of an SIA should grasp the concerns of the affected citizens. However, both privacy and data protection are not only fundamental rights but are also highly complex concepts around which public opinion is diverse, fluid and often tied to other issues, as a review of some key surveys over the last years demonstrates.[35]

Public opinion and acceptance are shaping factors in the development and deployment of surveillance technologies and infrastructures. Certain systems and technologies are accepted as necessary or unproblematic, while others are greeted with suspicion and even provoke outrage. Understanding what drives public perception and opinion on surveillance technologies is thus important in the broader comprehension of surveillance systems generally. Moreover, public opinion should play a significant role in shaping policy, particularly policy that may impact social structures, or the principles according to which the society is organised.[36]

Whilst it cannot be said that there is one single public opinion on surveillance technologies, there are certain factors that can be seen to have a significant influence. First, demographic factors, such as culture and age, and individual outlook factors such as an individual's stance on related issues, are important and form the background to perception.[37] Second, the information, and the sources of information and their presentation and approach are important, particularly considering the novelty of certain technologies and the consequent and apparently widespread lack of first-hand experience of technologies.[38] Third, the nature and operation of the technology itself are important, not only for the immediate reaction and images they provoke, but also as a result of the amount and quality of reference points and templates for understanding they prompt.[39] Finally, the expectation of, and trust in, the institutional, technological and social systems in which the technology will operate, as well as the expectation of the performance and effect of the technology within these systems, are key.[40]

The range of new surveillance technologies and the difference in their operation makes it difficult to pinpoint universal attitudes. However, certain trends and factors in current opinion can be isolated. Perhaps the most significant of these is that public opinion often lacks a solid factual basis, founded on knowledge of the actual technologies. Broadly speaking, this can be partially attributed to the novelty of new surveillance technology which means that the public has not had time to solidify references and form templates through which to comprehend function and consequence, and partially to the complexity of the operation of the technology itself (knowledge and understanding of the technologies themselves are limited) and the environments in which it operates (the key background systems and information flows out of which dangers arise are often invisible and may be detached both geographically and, in terms of effect, conceptually from the technology itself).[41] This appears to lead to assumptions about operation and a distinct lack of conceptual clarity, even to the extent that distinct technologies, posing distinct questions, are often merged and confused in public consciousness.

Whilst there is an awareness of the potential and usefulness of surveillance in certain situations and particularly in recognised security hotspots, a recurring point in each survey is the uneasiness with which new surveillance technologies are considered and greeted even as they purport to answer supposedly critical and desired social needs.[42] This is partly due to the lack of technological understanding, but it is also due to the awareness that the proliferation and perceived deterministic use of technologies may be creating something more sinister and potentially threatening to fundamental social principles. First, there is uncertainty about the reasoning, necessity, and targeting behind much surveillance

35 The most prominent ones in Europe are: The Gallup Organization,'Data Protection in the European Union: Citizens' Perceptions' (2008) Flash Eurobarometer 225, Brussels; TNS Opinion & Social, 'Attitudes on Data Protection and Electronic Identity in the European Union' (2011) Special Eurobarometer 359, Brussels.

36 See Daniel J Solove, *The Digital Person* (New York University Press 2004).

37 TNS Opinion and Social (n 19); Minas Samatas, 'Studying Surveillance in Greece: Methodological and Other Problems Related to an Authoritarian Surveillance Culture' (2005) 3 Surveillance & Society 181; James Backhouse and Ruth Halperin, 'A Survey on EU Citizen's Trust in ID Systems and Authorities', FIDIS Deliverable 4.4 (London School of Economics and Political Science 2007); Oliver Murphy, 'A Surveillance Society: Qualitative Research Report', Report prepared for COI on behalf of ICO (Information Commissioner's Office 2007).

38 Anders Jacobi and Mikkel Holst, 'Synthesis Report – Interview Meetings on Security Technology and Privacy' (2008) PRISE Deliverable 5.8; Lee S Strickland and Laura E Hunt, 'Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions' (2005) 56 Journal of the American Society for Information Science and Technology 221.

39 Jacobi and Holst (n 38) 20. ORC International, 'Public Attitudes Toward the Uses of Biometric Identification Technologies by Government and the Private Sector', Summary of Survey Findings for SEARCH (2002).

40 Backhouse and Halperin (n 37); Mary J Culnan and Pamela K. Armstrong, 'Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: an Empirical Investigation' (1999) 10 Organization Science 104.

41 Petter Bae Brandtzaeg and Marika Lüders, 'Privacy 2.0: personal and consumer protection in the new media reality' (2009) Norwegian Consumer Commission, Oslo; Strickland and Hunt (n 38).

42 Jacobi and Holst (n 38) 23; Lieberman Research Group, 'UNISYS Security Index: UK' (2010) Unisys Corporation.

technology and the logic according to which it is alleged to achieve its stated ends. Second, there is fear about the alterations in power relations the technology could bring about both in the short term, due to the lack of transparency of operation and of operators, and in the future, due to the uncertainty as to the potential for function creep and the reshaping of key social relationships. Finally, at an individual level, general data processing and privacy fears, such as ID fraud and abuse of collected data, appear to be transferred onto the background of each technology.[43]

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.

Given the importance that public perception has on the acceptance of specific surveillance technologies by the general public, we conclude that citizens' views have to be a central element of any (privacy) impact assessment. Furthermore, the assessment scheme has to address all issues mentioned. It has to provide the information about the technology itself and the practice in which it is used in a way understandable for the layman. The assessment process has to unveil the often complex consequences that a particular security practice may have and which other stakeholder interests are involved.

Based on its research, analysis and findings to this point, the consortium then formulated three scenarios involving public acceptance of different surveillance technologies in different applications. The consortium held three workshops to consider the issues raised in the scenarios and how to address such issues. The next section describes this process.

Stakeholder consultations help in the assessment of surveillance systems

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. 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 (eg by means of an SIA). Invited participants included academics, policy-makers, and representatives from industry (including private companies and R&D specialists), public authorities, law enforcement, data protection authorities (DPAs), 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 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, where conflicts need to be resolved and the importance of engaging a sufficiently representative group of stakeholders in an SIA.

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. 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. The media often play a key role in these political mobilisations. News coverage has also contributed to a more critical public perception. Societal drivers included the need to efficiently deal with social changes. Most of the stakeholders in all three workshops shared the opinion that, beyond privacy and data protection, there were crucial societal benefits of surveillance technologies,

43 Backhouse and Halperin (n 37); Jacobi and Holst (n 38).

such as providing security, mobility, and health care. However, each of these benefits has to be part of an approach that does not undermine privacy.

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. All stakeholders agreed upon the importance of complying with data protection law when developing and deploying surveillance technologies. Law enforcement has to guarantee all constitutional freedoms, not just safety and security, so data protection and other fundamental rights must also be protected. Thus, surveillance operators must consider proportionality, transparency, adequacy and data ownership. However, the current legal framework in Europe allows exceptions to the protection of privacy in the public security field. CSOs felt that the rule of law was a less strong protection than public authority and law enforcement stakeholders claimed.

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. A point of discussion with regard to consent was that consumers often do not understand what happens to their data because of this lack of transparency. Yet there could be a 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 more tailored to consumers' needs.

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. Yet, individuals are not always passive subjects of surveillance and may resist surveillance in unexpected ways.

Five insights to inform impact assessments

From the workshop, the consortium developed five key insights relating to the study of smart surveillance and reflecting on what to derive from PIA in devising an SIA.

First, surveillance has to do with the activity of governing. Far from the popular, Orwellian representation of surveillance as an authoritarian and anti-liberal practice or as a romanticised cape-and-dagger activity, it is a routine and long-standing practice for public administration, law-enforcement and security bodies as well as for the private sector. The notion that we live in 'surveillance societies' might be an oversimplification, but it does convey the view that there is nothing exceptional to surveillance, and that in any case, it is by no means alien to liberal regimes.

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 towards prediction and its corollaries, including the increasing reliance on datamining 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.

Potential solutions to the challenges of smart surveillance

In all three workshops, stakeholders proposed possible solutions to better protect privacy and other fundamental rights given the proliferation of smart surveillance

technologies. Most stakeholders focused on possible solutions that more directly addressed the key terms of the privacy and security debate, such as the following.

Better enforcement of existing rules

Even before adoption of the proposed Data Protection Regulation, significant privacy and data protection rules already exist in current legislation to provide some protections from smart surveillance technologies. However, many workshop participants felt that these rules were not enforced strongly enough, and that better enforcement would have a positive impact on citizens' privacy. 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 to courts where they could challenge practices. 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.

- *Education*: consumer or citizen education emerged as an important way to improve protections for fundamental rights. 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. Law enforcement and police stakeholders also need better education about their role in protecting privacy and personal data.
- *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.
- *Self-regulation*: representatives of industry were particularly keen to support self-regulatory initiatives. However, a representative from a consumer rights organisation argued that self-regulation should not be used at all, because it does not work.
- *Privacy impact assessment*: the co-regulatory PIA model was discussed in all three workshops. The proposed Data Protection Regulation contains a provision for data protection impact assessment (DPIA). A DPA representative offered data protection and PIAs as tools 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. If civil society organisations are not able to fully and fairly engage, there is a risk that PIAs will lack credibility. 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.

The scenario workshops provided the footing for the final phase of the SAPIENT project, ie developing and testing an SIA. The workshop delineated the issues that should or could be considered in an SIA and underscored the importance of engaging a wide range of different stakeholders in the process.

Developing an SIA

A principal goal of the SAPIENT project was to develop and test an SIA. To that end, the consortium first examined the state of the art in PIA to see what lessons or best practices could be applicable to an SIA methodology. The SAPIENT consortium reviewed the existing PIA methodologies, notably those used in Australia, Canada, France, Ireland, the Netherlands, New Zealand, the USA, UK[44] 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 are respecting the privacy of the citizens, (2) to limit the collection and storage of unnecessary data, and (3) to find a balance between data collection needs and data protection and privacy. The consortium also analysed examples of PIAs targeted at surveillance technologies and applications. On the other hand, it was also important to understand the limits of already existing PIA methodologies, and to check them against the features and the challenges of present and prospective smart surveillance technologies and practices. Surveillance systems and technologies have particularities that go beyond PIAs. In many cases (eg 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 (eg 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

44 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.

while analysing the impacts of these technologies or practices.

The consortium extracted the best elements and identified the main limits of existing PIAs and formulated a set of recommendations for an SIA methodology for the EU.

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

An SIA is more than a PIA

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 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 an SIA 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*, ie impacts. An SIA should include stakeholder consultation and, ultimately, lead to remedial actions as necessary 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.

The SIA process

An SIA may be undertaken (1) by those developing surveillance systems or technologies, (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:

- Surveillance systems should comply with the law.
- Surveillance should be used only when there are no more cost-effective alternatives.[45]
- 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.
- Mass surveillance systems should be subject to regulatory approval before deployment—ie 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.

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

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

An SIA should be regarded as a *process*, comprising the steps listed below.[46] 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.[47] A high-level overview is given below, and illustrated in Figure 1.

The list of the key steps for the SIA follows:[48]

- Phase I: Preparation
  1. Determine whether an SIA is necessary.
  2. Develop terms of reference for the surveillance assessment team.
  3. Prepare a scoping report. (What is the scope of the surveillance system?)
  4. Check compliance with legislation.
  5. Identify key stakeholders.

- Phase II: Risk identification and analysis
  6. Initiate stakeholder consultation.
  7. Identify risk criteria.
  8. Identify primary assets and feared events. (What could happen if the surveillance system is implemented?)
  9. Analyse the scope of feared events.
  10. Analyse the impact of feared events.
  11. Identify supporting assets.
  12. Identify threats and analyse vulnerabilities.
  13. Identify threat sources and analyse capabilities.
  14. Create a risk map (for prioritising risks for treatment).

- Phase III: Risk treatment and recommendations
  15. Risk treatment identification and planning
  16. Prepare an SIA report.
  17. Record the implementation of the report's recommendations.
  18. Publish the SIA report.
  19. Audit the SIA.
  20. 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. A streamlined 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.

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

46 This surveillance impact assessment guidance draws on D Wright and K Wadhwa, 'A Step-by-step Guide to Privacy Impact Assessment' (2012) Second PIAF workshop, Sopot, Poland, ISO 27005, ISO 31000, CNIL's privacy risk methodology, ENISA's risk management guidance, NIST 800–30 and EBIOS.

47 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, Energy Networks Association (2011) 23; Department of Energy and Climate Change (DECC), Smart Metering Implementation Programme—Privacy Impact Assessment (2012).

48 For a more comprehensive description of the assessment process, see David Wright and Charles Raab, 'Constructing a Surveillance Impact Assessment' (2012) 28 *Computer Law & Security Review* 613; David Wright and others, ''Integrating Privacy Impact Assessment in Risk Management' (2014) 4 International Data Privacy Law 155; David Wright, 'Making Privacy Impact Assessment More Effective' (2013) 29 The Information Society 307.

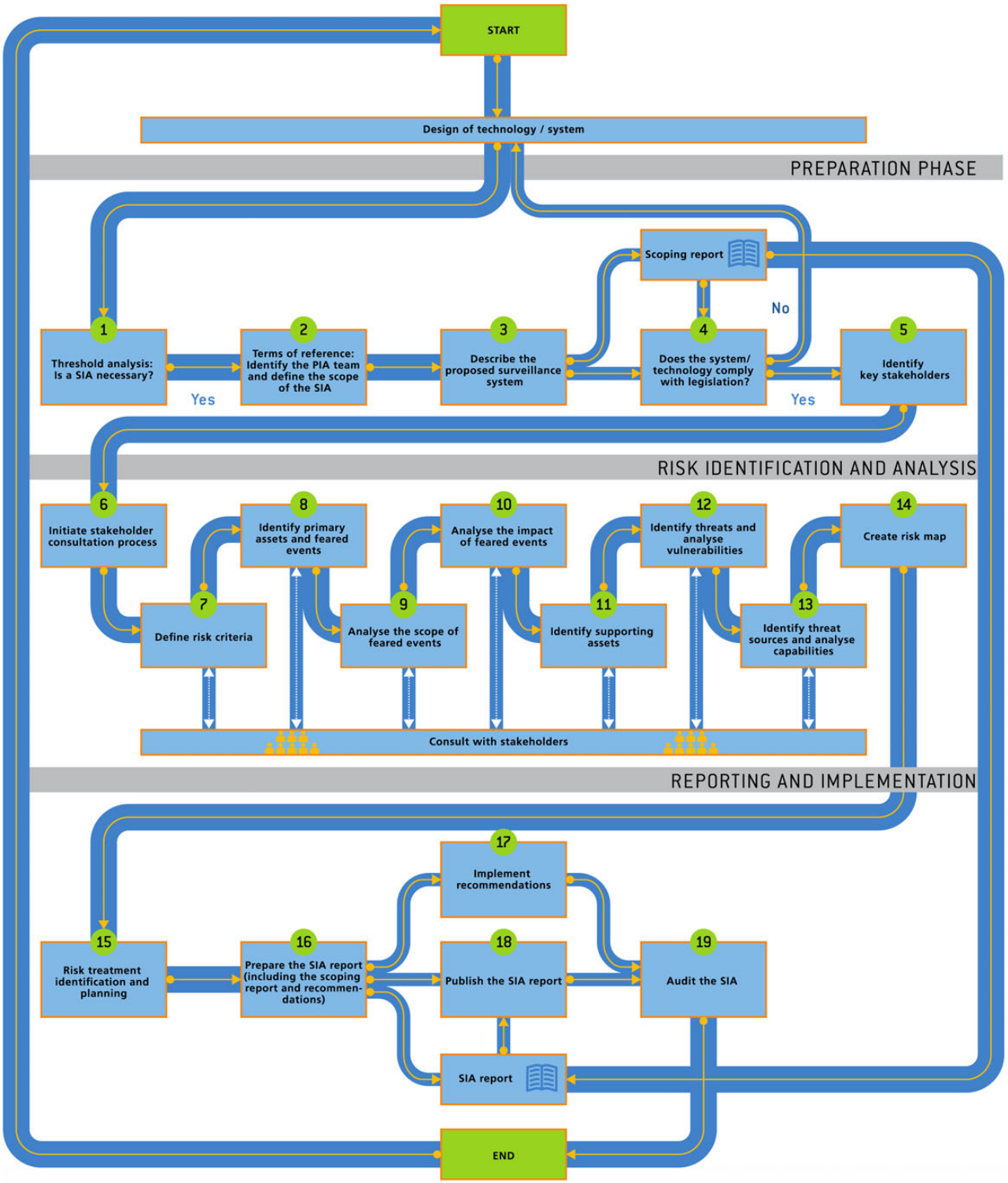

Figure 1. Impact assessment process.

- 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 is 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 SIAs. 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.

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). In 2009, 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. In February 2014, 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,[49] 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.

doi:10.1093/idpl/ipu027
Advance Access Publication 3 November 2014

49 Rachel Finn, David Wright and Michael Friedewald, 'Seven types of privacy', in S Gutwirth, R Leenes, P De Hert and others (eds), *European data protection: coming of age?* (Springer 2013) 3.