Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Constructing a surveillance impact assessment

David Wright [a], Charles D. Raab [b]

[a] Trilateral Research & Consulting, London, UK
[b] School of Social and Political Science, University of Edinburgh, UK

Keywords:
Surveillance impact assessment (SIA)
Privacy impact assessment (PIA)
Stakeholder consultation
Types of privacy
Types of surveillance

ABSTRACT

This paper describes surveillance impact assessment (SIA), a methodology for identifying, assessing and resolving risks, in consultation with stakeholders, posed by the development of surveillance systems. This paper appears to be the first such to elaborate an SIA methodology. It argues that the process of conducting an SIA should be similar to that of a privacy impact assessment (PIA), but that an SIA must take account of a wider range of issues, impacts and stakeholders. The paper categorises the issues and impacts to be considered in the conduct of an SIA and identifies the benefits of a properly conducted SIA.

1. Introduction

In spite of the prevalence of surveillance in our modern society, it is surprising that no one has yet developed a method for assessing the impact of surveillance on society. There could be several reasons for this. Perhaps regulators, privacy advocates and academics have felt that a *privacy* impact assessment (PIA) is sufficient for identifying and analysing the impacts of surveillance. But this would be an error, since a PIA would not catch all of the implications raised by a surveillance project. A PIA focuses on privacy, and while we can agree with Daniel Solove, who describes privacy as "encompassing (among other things) … freedom from surveillance"[1], surveillance impacts other values in addition to privacy. Furthermore, surveillance affects not only individuals, but also groups and society as a whole. Raab and Wright make this point and, in doing so, advocate extending the limits of PIA so that it considers values in addition to privacy and impacts not only on individuals, but also on groups and society as a whole.[2]

As of June 2012, the term "surveillance impact assessment" did not show up on the Social Science Research Network (SSRN). Ten instances showed up on Google Scholar, and of those, four were irrelevant (despite "surveillance impact assessment" being in quotes, four of the results contained a comma after surveillance and concerned grasslands, rodents, oil spills and oncology). The remaining citations referred to A *Report on the Surveillance Society*, prepared by the Surveillance Studies Network for the UK Information Commissioner's Office.[3] The earliest use of the term thus appears to be in 2006.[4]

The *Surveillance Society* report discusses surveillance impact assessment (SIA) in its last five pages. Although it gave a few examples of what an SIA would require, it was unable within the confines of the report to demonstrate at length how an SIA would be put into practice.

Little use appears to have been made of the term since then, at least not until the SAPIENT project, funded by the

[1] Solove, Daniel J., *Understanding Privacy*, Harvard University Press, Cambridge MA, 2008, p. 1.

[2] Raab, Charles, and David Wright, "Surveillance: Extending the limits of privacy impact assessment", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, pp. 363–383.

[3] Surveillance Studies Network (SSN), *A Report on the Surveillance Society*, prepared for the Information Commissioner, September 2006. http://www.ico.gov.uk/Global/Search.aspx?collection=ico&keywords=surveillance+report.

[4] Privacy impact assessment investigates the impact of technologies and systems on privacy. It should follow linguistically that surveillance impact assessment should investigate the impact of technologies and systems on surveillance, but this is obviously incorrect. Rather than change the terminology, we retain it here, where we take "surveillance impact assessment" to mean the assessment of surveillance on individual rights (including privacy) as well as on a range of social and other processes and values.

0267-3649/$ – see front matter © 2012 David Wright & Charles D. Raab. Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.clsr.2012.09.003

European Commission's Directorate General Enterprise, proposed the development of a surveillance impact assessment methodology. The three-year project began in March 2011.[5] The SAPIENT consortium is constructing a privacy impact assessment framework designed to address the particularities of existing and envisioned smart surveillance systems, technologies, projects and policies. To that end, it is extracting the best elements of existing PIA methodologies in order to construct a surveillance-suitable PIA framework, which it will field test on three different surveillance projects, the first time this will happen at European level.

Hence, there seems to be a case for developing a surveillance impact assessment methodology (or an "extended" PIA) that could be applied whenever a new surveillance project is contemplated or when an existing surveillance system is to be modified or expanded. Such a methodology could be used by the surveillance project manager, or a regulator could oblige the project manager to undertake an SIA.

2. Previous research

In constructing a surveillance impact assessment, we take note of previous papers of relevance.

Since the aforementioned *Surveillance Society* report appears to contain the first reference to surveillance impact assessment, it is logical to start there.[6] Although its discussion of an SIA is succinct, it is germane. Perhaps its most important finding in the context of this paper is that an SIA needs to take into account more than just privacy impacts: "To encompass the potentially harmful effects of surveillance on a wider basis than that of protecting privacy, it would be necessary to develop PIA tools beyond their existing configuration, and to develop what could be called surveillance impact assessment, or SIA… Because PIA has been innovated as a tool for looking at privacy, conceived in terms of individual rights, it is not at present best suited to embrace the further ramifications of surveillance in terms of a range of other social and personal impacts."[7]

While the *Surveillance Society* report appears to have coined the term SIA, others had already contested that adequate consideration of surveillance schemes had to go beyond privacy. Gary T. Marx argued in 1998 that the model of fair information principles was not adequate for addressing surveillance and that a more encompassing framework was needed[8]:

> *The Principles of Fair Information Practice are almost three decades old and need to be broadened to take account of new technologies for collecting personal information such as drug testing, video cameras, electronic location monitoring, and the Internet. I argue that the ethics of a surveillance activity must be judged according to the means, the context and conditions of data collection, and the uses/goals.*

He noted that:

> *underlying these questions are a cluster of value justifications. The most overarching and important is the Kantian idea of respect for the dignity of the person. When the self can be technologically invaded without permission and even often without the knowledge of the person, dignity and liberty are diminished. Respect for the individual involves not causing harm, treating persons fairly through the use of universally applied valid measures, offering meaningful choices, and avoiding manipulation and coercion. These in turn depend on being adequately informed.*[9]

In 2002, commenting on the significant increase in the use of technology for the discovering of personal information, Marx said that "[i]n a striking innovation, surveillance is also applied to contexts (geographical places and spaces, particular time periods, networks, systems and categories of person), not just to a particular person whose identity is known beforehand."[10] He also observed that "self-monitoring" has emerged as an important theme in the new surveillance. Computing plays an important role in the new surveillance, as Marx notes: "much modern surveillance also looks at settings and patterns of relationships".[11] Roger Clarke coined the term "dataveillance" to describe this phenomenon of the uses of databases of personal information in a paper predating by a decade those of Marx.[12]

In addition to the ethical impacts of surveillance, Marx also commented on the social impacts. He made the point that new surveillance technologies

> *create a potential for a very different kind of society [and] can call for stringent vigilance. In extending the senses (the ability to see in the dark, into bodies, through walls and over vast distances etc.) they challenge fundamental assumptions about personal and social borders (these after all have been maintained not only by values and norms and social organisation, but by the limits of technology to cross them). Low visibility and the involuntary and remote nature of much contemporary surveillance may mean more secrecy and lessened accountability, less need for consent and less possibility of reciprocity. Lesser costs create a temptation to both widen the net and thin the mesh of surveillance. For example what if brain scan technology lives up to the claims of its advocates to identify what people feel, know or are thinking?*

[5] www.sapientproject.eu. One of the partners in SAPIENT is David Wright, who also co-authored a chapter (see fn 2) on surveillance and privacy impact assessment with Charles Raab, who was a principal author of the *Surveillance Society* report for the ICO. In particular, Raab drafted "Part D: Regulating the Surveillance Society", pp. 76–98, on which this paper draws.

[6] See also Raab, Charles D., "Researching the Regulation of Surveillance", paper presented at the Conference on *The New Surveillance – A Critical Analysis of Research and Methods in Surveillance Studies*, Centre for Technology and Society, Technical University of Berlin, Berlin, 30 November–1 December 2006, especially pp. 14–17. This unpublished paper is available from the author.

[7] Surveillance Studies Network, p. 97.

[8] Marx, Gary T., "Ethics for the New Surveillance", *The Information Society*, Vol. 14, No. 3, 1998, pp. 171–185 [p. 172].

[9] Marx, 1998, p. 183.

[10] Marx, Gary T., "What's New About the 'New Surveillance'? Classifying for Change and Continuity", *Surveillance & Society*, Vol. 1, No. 1, 2002, pp. 9–29 [p. 10].

[11] Marx, 2002, p. 12.

[12] Clarke, Roger, "Information Technology and Dataveillance", *Communications of the ACM*, Vol. 31, No. 5, May 1988, pp. 498–512.

(New York Times, 9 Dec. 2001). In the interest of preventing terrible things from happening (which after all it would be irresponsible not to do, not to mention legal liability), the sacred value traditionally placed on interior life would be eroded.[13]

Surely, the potential for a very different kind of society has already been realised, i.e., we already live in a surveillance society, as Marx himself described it.[14] We can characterise a surveillance society as one wherein surveillance is pervasive, bringing the vast majority (if not all) of the population under surveillance, where a wide range of technologies is used for a wide variety of surveillance applications, and where the impacts of surveillance are also wide-ranging, well beyond those on privacy.

3. Similarities and differences between a PIA and an SIA

A surveillance impact assessment, as conceived in this paper, has several similarities to and differences from a PIA. There are many different PIA methodologies and their number seems to be growing bigger all the time. Hence, for the purpose of this paper, we refer to the PIA process advocated in the EC-funded PIAF project, which draws on the best of existing PIA methodologies.[15] The SIA methodology described here has been developed for the SAPIENT project[16] and seems to be the only extant one.

3.1. *Similarities*

A PIA and an SIA should follow a similar process. In the PIAF project, we identified 16 steps in the PIA process, as follows, all or most of which should apply in an SIA. Each of these steps is detailed in the paper referenced in footnote 15.

1. *Determine whether a PIA (or SIA) is necessary (threshold analysis).*
2. *Identify the PIA (or SIA) team and set the team's terms of reference, resources and time frame.*
3. *Prepare a PIA (or SIA) plan.*
4. *Determine the budget for the PIA (or SIA).*
5. *Describe the proposed project to be assessed.*
6. *Identify stakeholders.*
7. *Analyse the information flows and other impacts.*
8. *Consult with stakeholders.*
9. *Determine whether the project complies with legislation.*
10. *Identify risks and possible solutions.*
11. *Formulate recommendations.*
12. *Prepare and publish the report, e.g., on the organisation's website.*
13. *Implement the recommendations.*
14. *Ensure a third-party review and/or audit of the PIA (or SIA).*
15. *Update the PIA (or SIA) if there are changes in the project.*
16. *Embed privacy awareness throughout the organisation and ensure accountability.*

In sum, an SIA, like a PIA, should be a process of engaging stakeholders in order to identify the impacts on privacy and other values of a new project, technology, service or other initiative in order to take remedial action to minimise, avoid or overcome the risks.

3.2. *Differences*

Although a surveillance impact assessment should follow a *process* similar to that of a privacy impact assessment, the scope of an SIA is wider than that of a PIA, as Raab and Wright have explained.[17] In the same vein, Priscilla Regan has argued that

[d]efining contemporary problems associated with governmental and nongovernmental activities of monitoring and recording peoples' actions, behaviours and communications is best done by speaking in terms of 'surveillance' not 'privacy invasion'… The phrase 'privacy invasion', as it is commonly used and understood, is too limited to encompass what has become a distinguishing and disquieting feature of modern life. Surveillance as a concept, as an image, more accurately connotes the modern landscape.[18]

The principal differences between an SIA and a PIA are as follows:

First, while a PIA is principally concerned with the impacts of a project or technology or service on privacy, an SIA must address the impacts of a surveillance project not only on privacy, but also other issues and impacts – social, economic, financial, political, legal, ethical and psychological.
Second, an SIA is principally focused on groups or society as a whole. While a PIA may also consider societal effects of

[13] Marx, 2002, p. 16.
[14] In its Closing Communiqué of the 28th International Conference of Data Protection and Privacy Commissioners, held in London, 2–3 November 2006, the Commissioners made a virtually identical observation: "The 'Surveillance Society' is already with us."
[15] Wright, David, and Kush Wadhwa, "A step-by-step guide to privacy impact assessment", Presentation paper for the second PIAF workshop, Sopot, Poland, 24 April 2012. www.piafproject.eu. PIAF was co-funded by the European Commission's Directorate General Justice under its Fundamental Rights and Citizenship (FRC) programme (Grant JUST/2010/FRAC/AG/1137 30-CE-0377117/00-70). The project started in January 2011 and concluded in October 2012. It included a review of existing privacy impact assessment policy and practice in Australia, Canada, Hong Kong, Ireland, New Zealand, the UK and US to identify the best elements of each which could be incorporated in a PIA framework in the EU and Member States. The project had three partners, one of which is Trilateral Research & Consulting, represented by the author of this paper.
[16] SAPIENT is a 36-month collaborative research project (Project number: 261698) which aims to help policy-makers, technology developers and other stakeholders to better understand how and when smart surveillance should be used and to apply criteria to assure that such systems respect the privacy of citizens. The project, funded by the European Commission's Directorate General Enterprise, has eight partners, including Trilateral, represented by the author of this paper.
[17] Raab and Wright, 2012.
[18] Regan, Priscilla M., "Response to Bennett: Also in defence of privacy", *Surveillance & Society*, Vol. 8, No. 4, 2011, pp. 497–499 [p. 497].

privacy intrusions caused by a new technology, project or service, its starting point is the individual. (Gary T. Marx has noted that whereas the "old" surveillance involved "close observation, especially of a suspected person", the "new surveillance" targets whole groups and populations.[19])
Third, because an SIA must address a wider range of impacts, so too must it consult and engage with a wider range of stakeholders than a PIA.

4. Constructing a surveillance impact assessment

The bedrock of a surveillance impact assessment is identifying and describing the surveillance technologies to be developed and deployed in a new project; dealing with the issues to which the proposed surveillance gives rise; considering the impacts, of which there could be several, that the technologies or systems may have; and identifying and engaging with the stakeholders affected by or who have an interest in the surveillance project.

4.1. *Types of surveillance*

Just as a PIA should question all types of privacy-intrusive technologies and systems, an SIA should question all types of surveillance. While there are many different surveillance technologies, they can essentially be grouped within nine main types of surveillance, as follows:

Covert or visible – Some surveillance may be covert (e.g., eavesdropping or intercepts by the police) while other surveillance technologies (e.g., video cameras) may be visible. Some surveillance, e.g., the data mining by Google, Facebook and many others may also be invisible to users, although it may be possible to turn off some of it, for example, as a result of "Do not track" policies in the US.
Personal or mass surveillance – Clarke distinguished two main types of surveillance: "Personal surveillance is the surveillance of an identified person. In general, a specific reason exists for the investigation or monitoring. It may also, however, be applied as a means of deterrence against particular actions by the person, or repression of the person's behaviour. Mass surveillance is the surveillance of groups of people, usually large groups. In general, the reason for investigation or monitoring is to identify individuals who belong to some particular class of interest to the surveillance organisation. It may also, however, be used for its deterrent effects."[20]
Watching (visual surveillance) – includes technologies such as photography (cameras, mobile phones, mobile video), CCTV, unmanned aerial vehicles (drones), imaging scanners and high resolution ("keyhole") satellites.
"Listening" (communication surveillance) – includes audio recording devices such as those used to intercept wired and wireless communication (mobile telephony) as well as calls using Voice-over-Internet Protocol (VoIP). Call logging often provides surveillants with as much helpful information as eavesdropping does. The EU Data Retention Directive[21] requires electronic communications operators to retain call data (including e-mail data) for up to two years, which greatly facilitates the work of law enforcement authorities. Law enforcement authorities in the US solicited the metadata of calls (who called whom, on what date, at what time, for how long did the call last, etc.) more than 1.3 million times in 2011.[22]
Detecting (sensors) – can range from traditional retail security systems at store entrances and exits or metal detectors to complex, recently developed explosives-"sniffing"[23] or behavioural sensors. Although each type of sensor often performs only one specific task, these sensing systems can be combined to consolidate a comprehensive, multi-modal system. Other detectors include heat detectors.
Biometrics – such as facial recognition, gait recognition, iris scanning and keystroke logging can be used in surveillance systems. Biometric details may also be stored in RFID chips embedded in passports and travel cards, which can be "read" or detected by readers at airports (for example).
Tracking through space (geotagging, location determination) – While a wide variety of location determination systems exists, all of them fall into three main classes of localisation techniques: (1) triangulation, (2) proximity sensing and (3) scene analysis. Some of the most prevalent location determination techniques include GPS, WiFi/cell phone and RFID.
Dataveillance – as noted above, Roger Clarke coined the term in 1988. He defined it as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons. Dataveillance is significantly less expensive than physical and electronic surveillance, because it can be automated. As a result, the economic constraints on surveillance are diminished, and more individuals, and larger populations, are capable of being monitored."[24] Dataveillance includes data mining, data matching, data fusion and data aggregation, and is more or less synonymous with cyber surveillance.

[19] Marx, 2002.
[20] Clarke, 1988.
[21] European Parliament and the Council, Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Brussels, 15 March 2006.
[22] "In the first public accounting of its kind, cellphone carriers reported that they responded to a startling 1.3 million demands for subscriber information last year from law enforcement agencies seeking text messages, caller locations and other information in the course of investigations." Lichtblau, Eric, "More Demands on Cell Carriers in Surveillance", *The New York Times*, 8 July 2012.
[23] There are two main types of "sniffing" to detect explosives and drugs. Bulk detection involves non-olfactory methods to sense significant quantities of the targeted material. The technologies used for bulk detection of explosives or drugs are the same as the imaging scanners, i.e., X-ray backscatter imaging, millimetre wave imaging and terahertz imaging. "Chemical sniffers" or "electronic noses" detect and identify residual traces that indicate either the presence of, or someone's recent contact with, certain chemicals, such as drugs or explosives.
[24] Ibid.

Assemblages – refers to the convergence and combination of hitherto distinct surveillance technologies.[25] They greatly increase the power and capabilities of surveillance technologies. Assemblages are almost always examples of smart surveillance.[26]

4.2. Issues and impacts

The development and deployment of surveillance systems raise various issues and may have various impacts in individual privacy, social, economic, political, legal, ethical and psychological domains. A good surveillance impact assessment methodology should identify and consider how to address these various issues and impacts. The issues and impacts of interest to be addressed by the SIA in any particular instance will depend on contextual factors, such as the scale of the system to be deployed, the technologies to be used, the purpose of the surveillance, where and when it will be deployed, and so on. Different surveillance systems will raise different issues and have different impacts. In this section, we identify and briefly describe some of them. In doing so, we caution the reader that some issues and impacts can be categorised in more than way. For example, autonomy and dignity may be regarded as privacy issues, but they may also be regarded as ethical issues. Hence, the categories of issues and impacts delineated below should not be viewed as necessarily mutually exclusive; particular issues and impacts could be placed under more than one heading.

In the analysis employed by SIA, it should be borne in mind that restrictions on surveillance can have unintended consequences as well as those that are intended. Criminals and other evil-doers may cheer on privacy advocates who seek to limit the reaches of surveillance. Secrecy is just as important to criminals as it is to privacy advocates. Thus, to the extent that privacy advocates, civil-society organisations, the courts and others are able to curtail surveillance, their efforts could have the unintended consequence of helping criminals. Hence, assessors should ask: Does the project or technology have some consequences other than the purpose for which it is being deployed? That said, we now turn to consider the various issues and impacts to which surveillance gives rise in the categorical domains identified above.

4.2.1. Individual privacy issues and impacts

The most obvious impact of surveillance technologies is on privacy. As mentioned above, Daniel Solove describes privacy as a sweeping concept encompassing, among other things, freedom from surveillance. David Lindsay points out that privacy can be seen as a good in itself, as essential to our development as individuals, and is bound up with ideas of dignity, liberty and "personhood". It can also be justified for the individual on more instrumental grounds: without a degree of privacy, individuals cannot easily maintain a distinction between their personal and public lives, or exercise other important social and political rights, such as rights to freedom of religion, freedom of association and freedom of expression.[27] However, the intrinsic/functional distinction should not be too sharply drawn, because most defences of privacy embrace both emphases, while others have commented that privacy is *not* an antidote to surveillance.[28]

Surveillance systems and technologies – for the most part (an important qualification) – diminish, curtail, damage, intrude upon privacy. If surveillance systems monitor almost everything we do, where we go in the virtual and real worlds, what we buy, with whom we associate, what we say and (perhaps in the not too distant future) what we feel or think, then it undermines privacy. However, in some instances and not to be overstated, surveillance may actually protect privacy, especially the right to be let alone and to be safeguarded from bodily intrusion. For example, video cameras on the Underground may deter physical assaults on passengers.

Roger Clarke identified four categories of privacy, namely privacy of the person, privacy of personal behaviour, privacy of personal data and privacy of personal communication.[29] More recently, Finn, Wright and Friedewald have identified seven types of privacy.[30] In addition to Clarke's four types of privacy, they identified three other types, namely privacy of thoughts and feelings, privacy of location and space, and privacy of association (including group privacy). The assessor should investigate the impacts of surveillance on all seven types of privacy.

4.2.2. Social issues and impacts

Depending on the technologies employed and where and how they are deployed, surveillance practices can affect some individuals or groups more than others. Regulators, if not assessors, should consider a set of questions aimed at examining the social impacts, appropriateness and proportionality of a surveillance system before it is developed and deployed. Surveillance cameras and microphones in poor neighbourhoods can reinforce social stereotypes that the poor are

[25] Haggerty, Kevin D., and Richard V. Ericson, "The surveillant assemblage", *British Journal of Sociology*, Vol. 51, No. 4, 2000, pp. 605–622.

[26] Marx distinguishes between old or traditional surveillance and new or smart surveillance. See Marx, 2002. Wright et al. have defined smart surveillance "as being capable of extracting application-specific information from captured information (be it digital images, call logs or electronic travel records) in order to generate high-level event descriptions that can ultimately be used to make automated or semi-automated decisions". Wright, David, Michael Friedewald, Serge Gutwirth, Marc Langheinrich et al., "Sorting out smart surveillance", *Computer Law & Security Review*, Vol. 26, Issue 4, July 2010, pp. 343–354 [p. 347]. http://www.sciencedirect.com/science/journal/02673649.

[27] Lindsay, David. "An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law", *Melbourne University Law Review*, Vol. 29: 179, 2005 (online pagination: 1–45), Sections III-B and V-A. http://www.austlii.edu.au/au/journals/MULR/2005/4.html.

[28] Stalder, Felix, "Privacy is not an antidote to surveillance", *Surveillance & Society*, Vol. 1, No. 1, 2002, pp. 120–124.

[29] Clarke noted that, with the close coupling that has occurred between computing and communications, particularly since the 1980s, the last two aspects have become closely linked, and are commonly referred to as "information privacy". Clarke, Roger, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", Xamax Consultancy, Aug. 1997. http://www.rogerclarke.com/DV/Intro.html.

[30] Finn, Rachel, David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert et al., *European data protection: coming of age?*, Springer, Dordrecht, 2013 [forthcoming].

somehow more disposed to break the law than those with more means at their disposal. Coleman and McCahill argue that

> *Social impacts are evident on the life chances of those surveilled in terms of access and control over particular spaces, goods, services and upon particular working practices. Social impacts emanating from surveillance are also evident in terms of how societies come to understand, frame and respond to 'the crime problem' as well as the problem of 'victimhood'. These impacts may… reflect and reinforce relations of power that shape the habits and life chances of both 'the powerless' and 'the powerful'.*[31]

A similar sentiment can be found in the closing communiqué of the international conference, convened in London in 2006, of the world's data protection and privacy commissioners: "The effects of surveillance on individuals do not just reduce their privacy. They also can affect their opportunities, life chances and lifestyle. Excessive surveillance also impacts on the very nature of society…. More sophisticated approaches to regulation need to be adopted."[32]

The statement from the privacy commissioners echoes a similar comment in the *Surveillance Society* report issued that same year, and which was featured at the international conference: "Many surveillance practices have a direct effect on the nature of the society in which they are embedded, in terms of categorical discrimination (or empowerment), social exclusion, and other outcomes that would still be causes of concern even if the invasion of individual privacy were not in question."[33]

Other experts have also commented on the social impacts of surveillance. For example, Marx raises the caution that

> *[t]here is the possibility of becoming an even more stratified society based on unequal access to information in which individuals live in glass houses, while the external walls of large organizations are one-way mirrors. There is a significant (and perhaps growing) gap between the capabilities of the new surveillance technologies and current cultural, legal, and technical protections.*[34]

If surveillance systems can have such a deleterious impact on society, the assessor has to ask: Who authorised the system (e.g., Parliament) and how was it authorised? Has the system been the subject of public scrutiny (if not consensus)? Further questions are important as well: does the project, technology, application or service sort individuals into groups according to some predetermined profile that may advantage some groups and disadvantage others? Does the surveillance in question have a negative impact on social cohesion?

4.2.3. *Economic and financial issues and impacts*

Surveillance may raise economic and financial issues and/or have such impacts, which should be assessed. Some intelligence services and companies engage in industrial espionage in order to steal, appropriate or subvert intellectual property. Usually, such activity is covert, but occasionally comes to light, as it did when Google complained about Chinese surveillance and theft of its intellectual property.[35]

Identifying the economic and financial issues and impacts of surveillance systems should not only identify the costs of establishing the surveillance system, including the cost of the hardware, software and people, but provide a basis for considering more cost-effective alternatives or whether a surveillance system is necessary at all. For example, it has been reported that some 78 per cent of the UK's crime prevention activities in the 1990s was spent on CCTV[36] and yet the effectiveness of such surveillance has been repeatedly questioned, including in studies carried out by or for the police themselves.[37]

Surveillance systems are often expensive. Some assessment is needed to determine whether governments not only get value for money, but whether the surveillance system is actually the best way to achieve a given objective (e.g., a reduction in violent crime or in benefits fraud). The UK government is reportedly spending £2.5 billion to record communications traffic, but the likely cost-effectiveness of this has not been demonstrated.[38] Such expenditures also have an opportunity cost: perhaps the funds could be better spent in some other way, even within the criminal justice system.

Other economic aspects should also be considered; for example, Christian Fuchs and others have pointed out that many social networks, such as Facebook, take advantage of the free, unpaid labour of users to enrich their owners.[39]

---

[31] Coleman, Roy, and Michael McCahill, *Surveillance & Crime*, Sage, London, 2011, p. 113.

[32] 28th International Conference of Data Protection and Privacy Commissioners, Closing Communiqué, London, 2–3 November 2006.

[33] Surveillance Studies Network, p. 93.

[34] Marx, 1998, p. 183. See also Raab, Charles D., and Colin J. Bennett, "The distribution of privacy risks: Who needs protection?", *The Information Society*, Vol. 14, No. 4, October–December 1998, pp. 263–274; Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, The MIT Press, Cambridge, MA, 2006.

[35] Eunjung Cha, Ariana, and Ellen Nakashima, "Google China cyberattack part of vast espionage campaign, experts say", *The Washington Post*, 14 Jan 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359_2.html?sid=ST2010011300360.

[36] Surveillance Studies Network, p. 19. The *Surveillance Society* report cites as its source for this statistic Norris, Clive, and Gary Armstrong, *The Maximum Surveillance Society: The Rise of Closed Circuit Television*, Berg, Oxford, 1999, p. 54.

[37] See Welsh, Brandon C., and David P. Farrington, *Crime prevention effects of closed circuit television: a systematic review*, Home Office Research, Development and Statistics Directorate, August 2002; Gill, Martin, and Angela Spriggs, *Assessing the impact of CCTV*, Home Office Research, Development and Statistics Directorate, Feb 2005. The latter study concluded that, "[a]ssessed on the evidence presented in this report, CCTV cannot be deemed a success. It has cost a lot of money and it has not produced the anticipated benefits." See also *The Telegraph*, "One crime solved for every 1,000 CCTV cameras, senior officer claims", 24 Aug 2009. http://www.telegraph.co.uk/news/uknews/crime/6081549/One-crime-solved-for-every-1000-CCTV-cameras-senior-officer-claims.html.

[38] Gallagher, Ryan, "Why Does the U.K.'s New Internet Surveillance Plan Cost Nearly $4 Billion?", *Slate*, 18 June 2012.

[39] Fuchs, Christian, Kees Boersma, Anders Albrechtslund and Marisol Sandoval (eds.), *Internet and Surveillance*, Routledge, London, 2011.

4.2.4. *Political issues and impacts*

The development and deployment of a surveillance system may raise political issues and/or have political impacts. A key issue is how the electorate or consumers may view deployment of the surveillance system. Will they accept or reject it? If it is a covert system, how will the public react if news of its existence comes to light? Who has taken or will take the decision to deploy the system? To what extent have stakeholders been engaged in the decision-making process? How "fit for purpose" is the surveillance system? Public support for surveillance seems to depend in part on which surveillance technology is deployed and in what context. CCTV cameras in public spaces and transport systems seem to be acceptable to the public while large percentages of the UK, US and Australian populations oppose ID cards (even though ID cards are generally accepted in many other countries).

In addition to the political issues it may raise, a surveillance system could have political impacts, many of which arise from the way surveillance impacts privacy. Policy-makers and those planning to establish a new surveillance system should also consider the broader political impacts on democracy (or what is purported to be democracy). Does the technology "chill" freedom of speech and association (e.g., are "smart" CCTV cameras and/or microphones installed in public places able to eavesdrop on conversations of the public as distinct from specific suspects)? Citizens may be more circumspect about participating in protests if they know that the police will be able to identify them. They may avoid contact with certain groups if they believe they will be surveilled. They may feel inhibited in expressing their views if they feel those views could be held against them. The chilling effect of surveillance is invidious to a vibrant democracy. To assess the political impacts of a surveillance system, one should ask questions such as who is being surveilled by whom and for what purpose? Who has authorised the surveillance? Will the project or technology enhance the power of some at the expense of others? Who will have access to the data gathered by a surveillance system and how will such data be used? Will it undermine the electorate's trust in their elected officials? Will the surveillance system support or undermine democracy?

Not all surveillance has a negative political impact. A system that surveilled the banking industry might support democracy by making corporate wrong-doing harder to hide. Surveillance can also have a beneficial political impact on democracy where it detects electoral fraud, ballot-rigging, intimidation, etc. Gary T. Marx has observed: "Through offering high quality documentary evidence and audit trails, the new surveillance may enhance due process, fairness and legitimacy. It may contribute to the political pluralism central to democracy by making the tools of surveillance widely available so that citizens and competing groups can use them against each other, as well as government, to enhance accountability."[40]

4.2.5. *Legal issues and impacts*

The development and deployment of surveillance systems may also raise legal issues and have positive or negative legal impacts. There are different legal aspects to be considered.

First, a surveillance impact assessment, like a privacy impact assessment, should be more than simply a check that a particular scheme complies with relevant legislation. Nevertheless an SIA, like a PIA, should include an assessment that the proposed scheme does comply with the relevant legislation, for example, the EU Data Protection Directive or, in the UK, the Regulation of Investigatory Powers Act 2000. The 2006 *Report on the Surveillance Society* for the UK Information Commissioner opined that an SIA could assist an organisation in the "understanding of its own practices and how they can be improved in order to make them more compliant with the law, with codes of practice limiting surveillance, and/or with the image of integrity and trustworthiness that the organisation is trying to project".[41]

Second, a surveillance system that flouts the law can diminish respect for the law in at least two constituencies. Those who initiate a legally questionable system may feel free to install other such systems in the future, while those who see that some can establish such systems with impunity may feel they can ignore the law too. Where surveillance systems lack accountability and transparency, are implemented without due regard for the tests of necessity and proportionality, or are used in discriminatory ways against certain kinds of people, the principles of justice and the rule of law itself may be eroded.

Third, some surveillance systems are intended to catch those who commit offences, for example, those who exceed the speed limit or who assault other passengers on the Underground. Hence, in such cases, surveillance can support enforcement of the law.

4.2.6. *Ethical issues and impacts*

It is important to reiterate that some issues and impacts can be viewed from different perspectives – e.g., privacy or society or ethics; we have mentioned, for example, that other human values are frequently regarded as aspects of or closely related to privacy. However, they are also commonly regarded as ethical issues, especially where they are under pressure. Indeed, privacy itself can be regarded not only as a fundamental right and societal issue, but also as an ethical issue, as a recent report of the European Group on Ethics makes clear.[42] Certainly, the deployment of surveillance systems often raises ethical issues and, inter alia, may impact the autonomy or dignity of the individual as well as on social values beyond individual rights. Hence, a surveillance impact assessment should consider the ethical issues and impacts raised by the deployment of surveillance technology(-ies), amongst which are the following:

[40] Marx, 2002.

[41] Surveillance Studies Network, p. 95.

[42] EC President Barroso asked the European Group on Ethics in Science and New Technologies (EGE) to examine the ethical implications of information and communication technologies. In the course of their consequent report, the EGE refer to "the ethics dimension of privacy protection" and specifically to "individuals not consenting to the sharing of their own data. But in this last case, the absence of individuals' consent raises questions related to subjects' right to self-determination and autonomy and then are ethically sensitive." See EGE, Ethics of Information and Communication Technologies, Opinion of the European Group on Ethics in Science and New Technologies to the European Commission, No. 26, Brussels, 22 Feb 2012.

Autonomy – Does the project or new technology impact the autonomy, the freedom of choice or the freedom to be let alone, of the individual or group?
Dignity – Does the project or technology intrude upon the individual's dignity, as body scanning, fingerprinting and electronic tagging arguably do?
Informed consent – Have individuals freely given their explicit informed consent to being monitored, tracked and/or targeted?
Trust – Will the technology or project erode trust? Will groups or individuals believe they are not trusted by others, especially those who are in a stronger position of power?
Fairness – Are some groups treated differently from others? For example, corporate crime and workplace safety may be less surveilled than street crime, even though corporate malpractice may have much greater impacts.
Security – Is a new technology or project being introduced to improve security (and whose security is actually being improved)? How can we know if the claims of the security proponents are valid? Will a perceived increase in security take precedence over other values such as privacy? Who determines if security should take precedence?
Responsibility – Who will be accountable for ensuring that a surveillance impact assessment is properly conducted? Who will be responsible if a surveillance system is found to be unduly intrusive?
Harm – Will the surveillance system cause undue or unjustified harm to anyone (see below re psychological impacts)?
Justice (right of inspection and redress) – If the surveillance system is deployed, will the owner and/or operator provide those surveilled with a right of inspection of how their data or images are being used, stored, secured (and for how long)? Will those surveilled have a right of redress if their data or images are being used improperly or for purposes other than those originally specified?
Solidarity and benefit sharing – Will the technology or project erode social solidarity? Who benefits or loses from the surveillance scheme?

4.2.7. *Psychological impacts*

Surveillance technologies can have harmful psychological impacts on individuals, especially on individuals' sense of privacy. If people know that they are being surveilled, they are likely to be more cautious in what they say or do than they might otherwise be. This is the "chilling effect" seen from the standpoint of its psychological effect, not to mention its social effect. With ubiquitous surveillance, the citizenry may begin to feel they live in a police state or in some consumer hell as they are constantly bombarded with "personalised" advertising.

A surveillance system may also create embarrassment, shame, or otherwise put a person in a negative light, as Marx and others have noted.[43]

Marx has also noted that the concept of harm, whether in the collection or use of the data, can be made problematic: Should harm be measured objectively or subjectively, and how should we respond to individual and cultural differences in defining it?[44] Thus, what one might regard as a negative psychological impact, as a harm, may well depend on the context and who is deciding whether someone's claim of harm can be regarded as valid or not. Equally, how harmful something may be perceived to be is also context-dependent.

Some operators have turned surveillance into entertainment, for example, in the *Big Brother* and *I'm a celebrity… Get me out of here!* TV series. Similarly, Facebook users are encouraged to divest themselves of all sorts of personal information and photos of themselves and their friends. These ventures are insidious because, among other things, they condition people to believe that surveillance of others and of oneself is fun and harmless.

Surveillance systems might even have deleterious effects on the surveillants as well as the surveilled. Surveillants may distance themselves from those whom they surveil and become inured to the harm they cause others. Surveillance can have a dehumanising impact on both the surveillant as well as those surveilled.

4.3. *Stakeholders and surveillants*

An essential element in constructing a surveillance impact assessment is to identify the stakeholders and, especially, the surveillants among them. We define a stakeholder as someone who is interested in or affected by a particular system, technology, service, etc.[45] Thus, in some sense, even criminals can be regarded as stakeholders to the extent that they are the targets of surveillance or that they may use a surveillance technology to spy on and steal from someone or some organisation or group. Consultation with stakeholders is an important element of an SIA, as it is in a PIA; however, it would be quite understandable if it were normal practice for a surveillance project manager not to consult with criminals.[46]

It is important to identify the stakeholders and surveillants for at least three main reasons:

First, a conscientious surveillance project manager or SIA assessor will want to engage a representative cross-section of stakeholders in examining the privacy, social, economic, political, legal, ethical and psychological impacts and risks presented by a new surveillance project or technology and to profit from their ideas and suggestions on how to minimise or avoid or overcome those risks. There are various ways of engaging stakeholders – via surveys, workshops, focus groups, Delphis, interviews, online, consultative conferences, citizens' panels, etc. The point of an SIA consultation is not to take a vote of stakeholders on whether a given surveillance

[43] Marx, 1998, p. 182.
[44] Marx, 1998, p. 184.

[45] The EU guide to Eurojargon defines a stakeholder thusly: "Any person or organisation with an interest in or affected by EU legislation and policymaking is a 'stakeholder' in that process." http://europa.eu/abc/eurojargon/index_en.htm. We recognise, however, that if all may be considered stakeholders, that concept loses its distinctiveness and may thus not be useful in practice without further discriminations, which we suggest below; some stakes are bigger than, or different in many ways from, others.

[46] Nevertheless, there may be instances where consultation with those convicted of an offence might be in the public interest, e.g., when the criminal might be able to give evidence against other felons on how a surveillance system worked. For example, suppose a Chinese programmer defected and were able to give evidence to the West on the extent or aspects or targets of Chinese cyber espionage.

system is acceptable or not.[47] The point of the consultation is to identify risks and ways of overcoming those risks. Thus, it is in the assessor's interest to consult with as many different stakeholders as possible (within budgetary, practical or logistical constraints) because some stakeholders may be able to spot some risks overlooked by others. In many instances, the public will form an important stakeholder group. The views of the public may be obtained in different ways, e.g., through public opinion surveys or as mediated through civil-society organisations, such as consumer advocacy groups.

Second, the assessor should compile a list of stakeholders who could be impacted by the surveillance system or project. Some people or groups may be impacted more than or in ways different from others. The assessor should identify how these different groups could be impacted.

Third, the assessor should identify the surveillants, those who directly or indirectly are the instigators of the impacts on others. The assessor should understand the drivers or motivations of the surveillants, i.e., why are they establishing the surveillance system or supporting its establishment.

Among the potential surveillant stakeholders are the following:

Central governments – surveil their populations for taxation, border control, illegal immigration, benefits fraud, social services entitlement, social planning, census-taking, etc.

Local authorities – surveil their populations for transport policy and planning, local taxes (e.g., Council taxes), policing, etc.

Police – surveil individuals and groups for crime prevention, detection and apprehension. They may intercept individual phone calls, e-mails, Internet usage. They may use surveillance to engage in crowd control.

Telecom companies and Internet service providers – are obliged to retain data of our calls and e-mails for up to two years (in the EU).

Industry (manufacturers, integrators, suppliers) – have benefitted hugely from 9/11, the Madrid and London bombings and other terrorist acts. Surveillance and security budgets have grown exponentially in the past decade or so. Like weapons manufacturers and arms dealers who benefit from continuing hostilities between countries and peoples, the industry has a vested interest in the fear of terrorism and crime.

Banks – surveil existing and prospective customers to make sure we are not undue credit risks, but also to sell us new products. Bank transactions may also be legally required to be surveilled to the extent that criminals may use the banks for money-laundering or otherwise target the banks for exploitation.

Credit card companies – gather vast amounts of data from our purchases in order to target us better and to avoid ID fraud.

Credit reporting companies – such as Experian also gather vast amounts of personal information which they sell to third parties.

Insurance companies – amass personal data to assess the risk of insuring people according to predetermined profiles.

Social networks and other Web-based companies – profit from the free labour of users who post personal data and photos. Users provide the fuel for advertisers who are able to target users better and manipulate consumer behaviour.

Employers – surveil the workplace to maximise worker productivity, to detect theft or other insider threats, and to curtail negligence.

Health care providers – include doctors, hospitals, assisted living residences, medical trusts and researchers, electronic health record providers, among others, all of whom gather personal data (and sometimes anonymise it) to provide their services, sometimes in the interests of patients, sometimes in the interest of profit maximisation, sometimes in the interest of curtailing demands on the governmental budgets.

Schools, universities – capture personal data upon the enrolment of students and continue to capture data on the student's performance throughout his or her academic career.

Media – especially investigate and report on the activities of celebrities, politicians, sports stars, entertainers, etc., as well as on societal groups. The media influence the public perception of the acceptability of different forms of surveillance, but also sometimes reflect public perceptions. At times, the media have been overly intrusive and have been found guilty of hacking into private telephone calls.[48]

Foreign governments and industry – engage in espionage and disruption. Both may undertake clandestine activities to harvest proprietary information and, in so doing, to support their national industries at the expense of those based in other counties. They may also undertake these activities to gain some leverage in international negotiations or to disrupt some activities of which they do not approve. One's own government and domestic industries may also, of course, engage in these activities.

Criminals – monitor our movements to steal our property or extort money from us. Cyber criminals may employ botnets with thousands or hundreds of thousands of slave computers. We (or at least our computers) may be slaves without knowing so.

Family and friends – may surveil our opinions, movements, health, feelings and possibly even our thoughts. Parents may track the whereabouts of their children. Children may monitor the health of aged parents. We may reveal much about ourselves to family members and friends and they may be able to deduce even more.

Us – social media (Facebook, YouTube) have allowed ordinary people to become surveillants. New technologies (webcams, smart phones, dragonfly drones) enable the many to watch the few (the synopticon[49]). They also enable participatory surveillance where ordinary people contribute to their own surveillance. As mentioned above, reality TV shows such as *Big Brother* legitimise surveillance. As Pogo famously said

[47] The difficulties in arriving at a consensus or some other result are shared with other attempts at participatory democracy, including citizen juries and other forms of public engagement, but this is not the place to explore the literature on those initiatives.

[48] Agence France Presse (AFP), "Senior journalist implicated in hacking scandal: BBC", 14 Mar 2011. http://www.google.com/hostednews/afp/article/ALeqM5hO1soEGylWxJSqkgPahujetpxa2g?docId=CNG.9ef0a881a7c2cb5d9c21f0a1a7bdc17d.3e1.

[49] Mathiesen, Thomas, "The Viewer Society: Michel Foucault's 'Panopticon' Revisited", *Theoretical Criminology*, Vol. 1, No. 2, May 1997, pp. 215–234.

regarding humans' impact on the environment: "We have met the enemy and he is us." An SIA must consider the witting or unwitting involvement of the surveilled in surveillance practices.

Although the above is a relatively long list of stakeholders, it could be still more fine-grained and more segmented. The list is sufficient, however, to demonstrate the diversity of stakeholder groups, many of whom are likely to have differing views about particular surveillance systems, the risks they pose and possible measures to ameliorate those risks.

5. Questioning surveillance

A key feature in many PIA methodologies is the use of questions to help assessors and stakeholders to identify the impacts and risks that might accompany the development and deployment of a new system, technology, product or service. An SIA should follow a similar approach, even if some of the questions are different and more wide-ranging given the different types of surveillance technologies, the likely wider range of impacts and stakeholders, as discussed above.

As one can distinguish different types of surveillance, of surveillance technologies and of situations in which surveillance is applied or to be applied, the questions that one ought to ask in a SIA will also differ, at least to some extent. The 2006 *Report on the Surveillance Society* comments that "Any SIA, like any PIA, would have to be tailored to the specific characteristics of the practices or technologies in question, although there would be a broad, basic similarity among investigations across an array of practices, because they have much in common and because there are common legal or ethical requirements that they would have to meet."[50]

Marx's (1998) essay formulated 29 questions, mostly ethics-based, to ask in the consideration of a surveillance project.[51] Many others employ the use of questions to uncover the impacts of a new technology, product, service, programme or other initiative, including the socio-economic impact assessment formulated by the European Commission. The EC's first, fully developed impact assessment methodology was published in 2002 and the latest iteration was published in 2009. Many of the EC questions resonate with an SIA.[52]

An important question in any SIA is: who are the surveillants, who are they surveilling and why? Perhaps equally importantly, one ought to ask: Who is *not* being surveilled? Coleman and McCahill argue that "while it is often suggested that 'synopticism' has reversed hierarchies of surveillance by turning the 'surveillant gaze' on 'elites' and 'celebrities', even here media portrayals have a 'class-bias' which serves to reinforce existing divisions."[53] "While synoptic surveillance relies on a diet of the 'usual suspects', reinforcing common-sense ideas of 'crime' and 'social harm', it is also skewed by what this medium renders silent and leaves relatively invisible…. Corporate wrongdoing… hardly features in synoptic terms."[54]

Even more fundamental questions should be asked, derived from the ones that were indicated earlier. Are some racial, religious or socio-economic groups surveilled more than others? How have such surveillance practices been justified? Have stakeholders been consulted with regard to the establishment of the surveillance system? Have they been fully informed about the surveillance project? Is the surveillance project necessary at all? Will the process of conducting a surveillance impact assessment be transparent, i.e., will those involved in the SIA have the same information about the surveillance scheme?

Another set of questions to ask are these: Are there alternatives to the project or technology that are less intrusive upon an individual's rights or the impacts on society? Do the surveilled have alternatives or choices? For example, in order to board an aeroplane, a passenger may have to consent to a body scan. The only alternative in such a case may be not to fly, but this is not an effective choice.

6. Consulting stakeholders and publishing the results

As we have emphasised, an important element in constructing a surveillance impact assessment is consultation with stakeholders. Consultation is a way of engaging stakeholders in the process of determining whether a surveillance system is necessary; how it should be designed; what oversight should be put in place; whether the surveillance scheme is proportionate; and whether there are alternatives to achieve the same purpose. Stakeholders may bring new ideas and may help to identify risks and solutions. Engaging stakeholders is a way of minimising downstream liability, of conducting a beta test of a system, and of gauging public acceptability of a new system.

Many companies and governments will be against consultation because they fear criticism, or fear that competitors will learn what they are doing, or believe that a consultation might comprise security. Such concerns are often misplaced, or else solutions can be found to address such concerns, as discussed in the next section. Suffice it to say here, however, consultation has many benefits.

Similarly, once the assessor has finished her work, the report of the surveillance impact assessment should be published. The report could be published on the organisation's website and/or published on an official registry, whether this is established by government, the regulatory agency, a trade association or an NGO. Publication will support transparency, and will provide assurance that risks have been identified and solutions found to minimise, avoid or overcome those risks; or, perhaps in a worst-case scenario, the organisation has decided to accept the risk because it perceives the benefits to be greater. Publication will help raise the awareness of an organisation's staff as well as the public about how to conduct a proper SIA, and about the substantive issues surfaced by surveillance.

Publication of an SIA report will facilitate third-party review and/or audit of the report. Third-party review of the SIA has

[50] Surveillance Studies Network, 2006, p. 95.
[51] Marx, 1998.
[52] European Commission, Impact Assessment Guidelines, SEC(2009) 92, Brussels, 15 January 2009. http://ec.europa.eu/governance/impact/commission_guidelines/docs/iag_2009_en.pdf.
[53] Coleman and McCahill, p. 127.
[54] Coleman and McCahill, p. 126.

several purposes. First, it will help ensure that the SIA was conducted properly. Second, it will support accountability. Third, it will help ensure that the assessor's recommendations were actually implemented or, if some of them were not, it will investigate the reasons why they were not. Fourth, like publication, a third-party review will help to raise the quality of SIAs.

Consultation, publication and third-party review are the most contentious elements in an SIA, but they are essential if an SIA is to have credibility. Without these features, an organisation can perform the most perfunctory of SIAs and then claim that it has taken the public interest into account, when in fact it has not. Surveillance schemes and SIAs need oversight if they are not to have negative impacts, as identified above.

7. Arguments against surveillance impact assessment

Inevitably, some surveillants (government and industry) will argue against subjecting surveillance systems to an SIA. Among such arguments, Raab and Wright envisage the following (each of which is followed by a rebuttal)[55]:

7.1. An SIA would be a brake on technical progress

Some surveillants might argue that the conduct of an SIA could slow down or impede the development of surveillance technologies. Against this is the argument that to separate technical progress from other social phenomena is to create, without sufficient warrant or reason, a zone of exception in which other values cannot enter, thus altering the nature of society and the possibility of individual privacy through a form of political and economic fiat.

7.2. Some surveillance involves national security

As surveillance is often undertaken by law enforcement authorities and intelligence agencies in the interests of national security and the maintenance of public order, some might claim that an SIA would inhibit the efficiency and effectiveness of these functions. However, creating exceptions opens the door to abuse. Even the US Department of Homeland Security has recognised this in regard to privacy impact assessments, saying: "A PIA should be conducted for *all* systems handling personally identifiable information *including classified or law enforcement sensitive programs*."[56]

If security concerns are truly serious, these could be addressed by conducting an SIA with a non-disclosure agreement so that a representative group of stakeholders could be engaged in the process of assessing the surveillance impacts. Furthermore, budget submissions for new security initiatives could be accompanied by an SIA as a condition of funding. In Canada, government agencies must include a PIA with their budgetary submissions, and deputy ministers must approve the final PIA reports which must also be copied to the Office of the Privacy Commissioner of Canada.[57] The funding agency could be given the power to turn down a budgetary submission if it judged the SIA to be inadequate. The Treasury Board in Canada has such a power. Post-SIA audits carried out by an independent third-party could ensure the agreed SIA recommendations were actually implemented. Such measures could be put in place to ensure that new security initiatives were subjected to an SIA without actually compromising security.

7.3. Some surveillance involves commercial sensitivity

Companies could argue that for competitive reasons or in the interests of protecting intellectual property, at least some of their activities should not be subject to a SIA. However, the UK Information Commissioner's Office has addressed this argument and advises that sensitive details can be placed in a less widely distributed appendix and protected by confidentiality constraints (it counsels that such suppression should be limited to what can be justified).[58] Maintaining or increasing public confidence in the legitimacy of properly regulated surveillance is, after all, an important objective of an SIA.

7.4. Some surveillance involves more than one country

Surveillance is not just an activity conducted within the borders of one country. It has become a transnational practice. National security establishments deem some surveillance projects involving more than one country to be so secret they cannot be subject to discussion among stakeholders. Echelon, the spy satellite system operated by the US, UK, Canada, Australia and New Zealand, was kept secret from the public for many years.[59] However, ring-fencing such activities so that they are not subject to an SIA risks abuse, examples of which abound. The US government wanted access to the financial transactions made by millions of citizens in many countries and recorded by SWIFT. The US and SWIFT kept the access

[55] Raab and Wright, 2012. The authors postulate arguments against subjecting surveillance to a PIA, but the arguments are equally applicable to an SIA.

[56] Department of Homeland Security, *Privacy Impact Assessments: The Privacy Office Official Guidance*, Washington, DC, June 2010, p. 7; http://www.dhs.gov/files/publications/gc_1209396374339.shtm. Walter Peissl of the Austrian Institute of Technology Assessment, perhaps slightly cynically, argues that "More surveillance does not necessarily lead to more security. Rather, this equation seems to be a brilliant marketing trick of the law enforcement authorities around the world to get things going they had on their agenda for many years already." Peissl, Walter, "Surveillance and Security – A Dodgy Relationship", Institute of Technology Assessment, Vienna, January 2002. www.oeaw.ac.at/ita/pdf/ita_02_02.pdf; emphasis added.

[57] "Federal organizations seeking preliminary project approval (PPA) from the Treasury Board pursuant to the Project Management Policy must include the results of the Privacy Impact Assessment (PIA) in the body of the submission or project brief, where applicable." Treasury Board of Canada Secretariat, "A Guide to Preparing Treasury Board Submissions", Ottawa, 2002, Annex D, section 4. http://www.tbs-sct.gc.ca/pubs_pol/opepubs/TBM_162/gptbs-gppct09-eng.asp#d4. See also the TBS Privacy Impact Assessment Policy, section on accountability, 2 May 2002. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450&section=text.

[58] Information Commissioner's Office (ICO), *Privacy Impact Assessment Handbook*, Version 2.0, Wilmslow, Cheshire, June 2009, pp. 33, 34, 40.

[59] Page, Lewis, "Original 'Echelon' secret UK–US spookery treaty published", *The Register*, 25 June 2010. http://www.theregister.co.uk/2010/06/25/echelon_publication/.

secret for some years until *The New York Times* revealed what had been going on. SWIFT was censured and criticised by data protection authorities in Europe for releasing the data without, as a minimum, consulting the Belgian authority.

It could be argued that conduct of an international SIA would be difficult in procedural and organisational terms, as well as with regard to applicable law. However, the countries involved in an international surveillance operation could conduct their own SIA and, following its recommendations, negotiate with the other countries as necessary to ensure the surveillance operation was proportionate and necessary or whether certain measures could be undertaken to ensure that the operation was subject to the oversight of, for example, a parliamentary committee and/or a court of law. New Zealand's *Privacy Impact Assessment Handbook* foresaw this situation some years ago:

> *Certain projects will have significant privacy implications in more than one jurisdiction. Indeed, some initiatives will have truly global implications. In such cases, comment might be invited from the privacy commissioners of several countries before finalising the privacy impact report. A significant objective of a PIA in such projects may be to ensure that the project meets or exceeds the data protection and information privacy requirements in all the relevant countries and achieves a level of trust amongst consumers and regulators.*[60]

The message here is that transnational projects should not escape the scrutiny of a PIA (or an SIA), simply because they are transnational.

7.5. *An SIA might reveal practices of questionable effectiveness*

Officials may not want to subject surveillance projects to an SIA because they fear that some forms of surveillance can be questioned with regard to their effectiveness, especially after much public money has been spent. In the UK, as mentioned above, CCTV has been the single most heavily-funded crime prevention measure operating outside the criminal justice system. As also mentioned above, the two major studies funded by the UK Home Office came up with less than glowing reviews of the effectiveness of CCTV.[61] The police themselves have questioned the utility of CCTV. The head of London Metropolitan Police's Visual Images, Identifications and Detections Office (Viido), speaking at a conference in 2008, said the huge investment in closed-circuit TV technology had failed to cut UK crime. He described the CCTV system as an "utter fiasco".[62] Thus, some surveillance operators might wish to escape the scrutiny of an SIA not because of any inherent sensitivity of the project, but only because critics might call into question the wisdom of their decision-making.

8. The legitimacy (and benefits) of subjecting surveillance to an SIA

Against these arguments, we believe that subjecting surveillance projects and activities to an SIA yields benefits such as greater public accountability[63], greater public awareness of the consequences and impacts of surveillance, a reduction in unwarranted surveillance, and greater equilibrium in information and power asymmetries, among others.

An SIA provides a way of detecting potential privacy and other ethical problems and of taking precautions by building tailored safeguards before, not after, a surveillance operator makes heavy investments.[64] The costs of fixing a project at the planning stage will be a fraction of those incurred later on. If the surveillance impacts are unacceptable, the project may even have to be cancelled altogether. Thus, an SIA helps reduce costs in management time, legal expenses and potential media or public concern by considering risks and impacts early. It helps an organisation to avoid costly or embarrassing mistakes.

Although an SIA should be more than simply a compliance check, it does nevertheless enable an organisation to demonstrate its compliance with legislation in the context of a subsequent complaint, audit or compliance investigation. In the event of an unavoidable risk or breach occurring, the SIA report can provide evidence that the organisation acted appropriately in attempting to prevent the occurrence. This can help to reduce or even eliminate any liability, negative publicity and loss of reputation.[65]

An SIA enhances informed decision-making and exposes internal communication gaps or hidden assumptions about the project. An SIA is a tool to undertake the systematic analysis of privacy, ethical and other issues arising from a project in order to inform decision-makers. An SIA can be a credible source of information. It enables an organisation to learn about the pitfalls of a project directly, rather than having its critics or competitors point them out. An SIA assists in anticipating and responding to the public's concerns.

An SIA can help an organisation to gain the public's trust and confidence. Trust is built on transparency, and an SIA is a disciplined process that promotes open communications,

[60] Stewart, Blair, *Privacy Impact Assessment Handbook*, Office of the Privacy Commissioner, Auckland, June 2007, p. 14. http://privacy.org.nz/privacy-impact-assessment-handbook/A first edition of the Handbook appeared in 2002.

[61] Welsh, Brandon C., and David P. Farrington, Crime prevention effects of closed circuit. television: a systematic review, Home Office Research, Development and Statistics Directorate, August 2002; Gill, Martin, and Angela Spriggs, Assessing the impact of CCTV, Home Office Research, Development and Statistics Directorate, Feb 2005.

[62] BBC News, "CCTV boom 'failing to cut crime'", 6 May 2008. http://news.bbc.co.uk/1/hi/uk/7384843.stm.

[63] The *Surveillance Society* report, op. cit., p. 95, also says an SIA can be a mechanism for accountability: "One advantage that SIA could have is in assisting regulatory agencies and individual citizens to understand and control surveillance practices by making them more transparent and their proponents more accountable." It makes the point again in different words: "If SIAs were required of firms or public organisations and made public as the basis of further discussion as well as approval, they would play a part in opening up surveillance to public scrutiny and comment."

[64] These and other benefits of an SIA, as identified in this section, have been adapted from Wright, David, "The state of the art in privacy impact assessment", *Computer Law & Security Review*, Vol. 28, No. 1, Feb. 2012, pp. 54–61. http://www.sciencedirect.com/science/journal/02673649.

[65] Health Information and Quality Authority, *Guidance on Privacy Impact Assessment in Health and Social Care*, Dublin, December 2010, p. 14.

common understanding and transparency. An organisation that undertakes an SIA appropriately demonstrates that it takes societal concerns into account and that it wishes to avoid negative impacts. It demonstrates to its employees and contractors that it takes privacy and other social values seriously and expects them to do so too. An SIA is a way of educating employees about privacy and other social values and making them alert to problems that might damage the organisation. It is a way to affirm the organisation's values. An organisation may wish to use an SIA as a way to check out third-party suppliers, to verify that they will not create negative impacts.

A proper PIA demonstrates to an organisation's customers and citizens that it respects their privacy and is responsive to their concerns. Although there is no hard evidence of this, it is plausible that customers or citizens are more likely to trust an organisation that performs an SIA than one that does not, and that – other things in the market or citizen-state relationship being equal – they are more likely to take their business to an organisation they can trust than one they do not, or to feel confident in engaging in official transactions.

We assume regulators are likely to be more sympathetic towards organisations that undertake SIAs than those that do not. An SIA is a self- or co-regulatory instrument which may obviate the need for severe enforcement of "hard" law. Thus, if organisations are seen to carry out proper (full-blooded) SIAs, they may escape the more onerous burdens imposed by legislation. (However, this should not be taken as an argument against legislation and for self-regulation.)

Official regulators have often been taken unawares by business or governmental ICT or systems proposals that pose potential threats to privacy or that have ominous surveillance capabilities. Regulators, whether official or civil-society members of the privacy and surveillance policy community, may be sidelined from the policy and decision arenas in which these plans are developed and implemented, or may enter them too late to have influence upon them. PIA and SIA may help in fostering a more proactive regulatory approach, but only to the extent that access to policies and plans occurs early enough. As far as regulatory agencies are concerned, it would be helpful if their early intervention and scrutiny were supported by statute or other binding requirement.[66]

While there is a paucity, indeed a complete lack, of quantitative data on the cost-benefit of SIA, the benefits identified here suggest that a properly conducted SIA creates a win-win situation for most, if not all stakeholders.

9. Conclusion

This paper is the first detailed one to describe a surveillance impact assessment methodology. Despite the prevalence of surveillance in society, it seems curious that no one has constructed an SIA methodology until now. It may be that some have considered that a PIA is a tool sufficient for examining the prospects for surveillance systems. This paper has argued that as good as PIA is, it is not adequate to address the complexities of a surveillance system and that an SIA should be used. This is because surveillance systems have impacts wider than only those on privacy. Hence, the paper has identified the similarities and differences between a PIA and an SIA. While the *process* of conducting a PIA and an SIA are broadly similar, the surveillance impact assessor must take into account various impacts and factors that are typically absent from a PIA.

The paper has sketched the different types of surveillance, any one of which (or any combination of which) should be subject to an SIA. It has also identified the different types of impact that should be considered when conducting an SIA. It has described the SIA process and the various elements in an SIA. Consultation with stakeholders is an essential element of a proper SIA, and the paper has listed various groups of stakeholders who could be considered in an SIA. Questions are a useful device to uncover the impacts of a surveillance system as well as possible solutions. The paper has also made the case for consulting stakeholders and publishing the results. It has considered various arguments against SIA and has put forward counter-arguments. Finally, it has identified the benefits for stakeholders, including those wanting to deploy a system, of subjecting a surveillance system to an SIA before it is deployed.

[66] Surveillance Studies Network, p. 96.

Acknowledgement

This paper has been prepared based in part on research undertaken in the context of the SAPIENT project (Project number: 261698), funded by the European Commission's Directorate General Enterprise. The views expressed in this paper are those of the authors alone and are in no way intended to reflect those of the European Commission.

David Wright (*david.wright@trilateralresearch.com*) *Member, CLSR Professional Board, Managing Partner, Trilateral Research & Consulting, London.*

Charles D. Raab (*c.d.raab@ed.ac.uk*) *Professor of Government, School of Social and Political Science, University of Edinburgh.*

REFERENCES

28th International conference of data protection and privacy commissioners, closing communiqué, London, 2–3 November 2006. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/06-11-03_London_Communique_EN.pdf.

Agence France Presse (AFP). Senior journalist implicated in hacking scandal: BBC, http://www.google.com/hostednews/afp/article/ALeqM5hO1soEGylWxJSqkgPahujetpxa2g?docId=CNG.9ef0a881a7c2cb5d9c21f0a1a7bdc17d.3e1; 14 Mar 2011.

Bennett Colin J, Raab Charles D. The governance of privacy: policy instruments in global perspective. Cambridge, MA: The MIT Press; 2006.

BBC News. CCTV boom 'failing to cut crime', http://news.bbc.co.uk/1/hi/uk/7384843.stm; 6 May 2008.

Clarke Roger. Information technology and dataveillance. Communications of the ACM May 1988;31(5):498–512.

Clarke Roger. Introduction to dataveillance and information privacy, and definitions of terms. Xamax Consultancy, http://www.rogerclarke.com/DV/Intro.html; Aug. 1997.
Coleman Roy, McCahill Michael. Surveillance & crime. London: Sage; 2011.
Eunjung Cha Ariana, Nakashima Ellen. Google China cyberattack part of vast espionage campaign, experts say. The Washington Post, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359_2.html?sid=ST2010011300360; 14 Jan 2010.
European Commission. Impact assessment guidelines. SEC (2009) 92, Brussels, http://ec.europa.eu/governance/impact/commission_guidelines/docs/iag_2009_en.pdf; 15 January 2009.
European Group on Ethics in Science and New Technologies (EGE), Ethics of Information and Communication Technologies, Opinion of the European Group on Ethics in Science and New Technologies to the European Commission, No. 26, Brussels; 22 Feb 2012.
European Parliament and the Council. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Brussels; 15 March 2006.
Finn Rachel, Wright David, Friedewald Michael. Seven types of privacy. In Gutwirth Serge, Leenes Ronald, De Hert Paul, et al., editors. European data protection: coming of age? Dordrecht: Springer, forthcoming.
Fuchs Christian, Boersma Kees, Albrechtslund Anders, Sandoval Marisol, editors. Internet and surveillance. London: Routledge; 2011.
Gallagher Ryan. Why does the U.K.'s new internet surveillance plan cost nearly $4 billion? Slate, http://www.slate.com/blogs/future_tense/2012/06/18/communications_data_bill_and_the_cost_of_government_internet_surveillance_programs_.html?wpisrc=sl_ipad; 18 June 2012.
Gill Martin, Spriggs Angela. Assessing the impact of CCTV. Home Office Research, Development and Statistics Directorate; Feb 2005.
Haggerty Kevin D, Ericson Richard V. The surveillant assemblage. British Journal of Sociology 2000;51(4):605–22.
Health information and quality authority, guidance on privacy impact assessment in health and social care; December 2010. Dublin.
Information Commissioner's Office (ICO). Privacy impact assessment handbook. Version 2.0, Wilmslow, Cheshire; June 2009.
Lichtblau Eric. More demands on cell carriers in surveillance. The New York Times, http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?_r=1; 8 July 2012.
Lindsay David. An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law. Melbourne University Law Review 2005;29:179 (online pagination: 1–45), sections III-B and V-A. http://www.austlii.edu.au/au/journals/MULR/2005/4.html
Marx Gary T. Ethics for the new surveillance. The Information Society 1998;14(3):171–85, http://www.indiana.edu/~tisj/readers/toc/14.html.
Marx Gary T. What's new about the 'new surveillance'? Classifying for change and continuity. Surveillance & Society 2002;1(1):9–29.
Mathiesen Thomas. The viewer society: Michel Foucault's 'Panopticon' revisited. Theoretical Criminology May 1997;1(2):215–34, http://tcr.sagepub.com/content/1/2/215.abstract.
Norris Clive, Armstrong Gary. The maximum surveillance society: the rise of closed circuit television. Oxford: Berg; 1999.
Page Lewis. Original 'echelon' secret UK–US spookery treaty published. The Register, http://www.theregister.co.uk/2010/06/25/echelon_publication/; 25 June 2010.
Peissl Walter. Surveillance and security: a dodgy relationship. Vienna: Institute of Technology Assessment, www.oeaw.ac.at/ita/pdf/ita_02_02.pdf; January 2002.
Raab Charles D. Researching the regulation of surveillance. Paper presented at the conference on the new surveillance – a critical analysis of research and methods in surveillance studies. Centre for Technology and Society, Technical University of Berlin, Berlin, 30 November–1 December 2006.
Raab Charles D, Bennett Colin J. The distribution of privacy risks: who needs protection? The Information Society October–December 1998;14(4):263–74.
Raab Charles, Wright David. Surveillance: extending the limits of privacy impact assessment. In: Wright David, De Hert Paul, editors. Privacy impact assessment. Dordrecht: Springer; 2012. p. 363–83.
Regan Priscilla M. Response to Bennett: also in defence of privacy. Surveillance & Society 2011;8(4):497–9.
Solove Daniel J. Understanding privacy. Cambridge, MA: Harvard University Press; 2008.
Stalder Felix. Privacy is not an antidote to surveillance. Surveillance & Society 2002;1(1):120–4.
Stewart Blair. Privacy impact assessment handbook. Auckland: Office of the Privacy Commissioner. p. 14, http://privacy.org.nz/privacy-impact-assessment-handbook/; June 2007.
Surveillance Studies Network (SSN). A report on the surveillance society, http://www.ico.gov.uk/Global/Search.aspx?collection=ico&keywords=surveillance+report; September 2006. Prepared for the Information Commissioner.
Treasury Board of Canada Secretariat. A guide to preparing Treasury Board submissions. Ottawa, http://www.tbs-sct.gc.ca/pubs_pol/opepubs/TBM_162/gptbs-gppct09-eng.asp#d4; 2002.
The Telegraph. One crime solved for every 1,000 CCTV cameras, senior officer claims, http://www.telegraph.co.uk/news/uknews/crime/6081549/One-crime-solved-for-every-1000-CCTV-cameras-senior-officer-claims.html; 24 Aug 2009.
Treasury Board of Canada Secretariat. TBS privacy impact assessment policy, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450&section=text; 2 May 2002.
[US] Department of Homeland Security. Privacy impact assessments: the Privacy Office official guidance. Washington, DC. p. 7, http://www.dhs.gov/files/publications/gc_1209396374339.shtm; June 2010.
Welsh Brandon C, Farrington David P. Crime prevention effects of closed circuit television: a systematic review. Home Office Research, Development and Statistics Directorate; August 2002.
Wright David. The state of the art in privacy impact assessment. Computer Law & Security Review Feb. 2012;28(1):54–61, http://www.sciencedirect.com/science/journal/02673649.
Wright David, Wadhwa Kush. A step-by-step guide to privacy impact assessment. Presentation paper for the second PIAF workshop, Sopot, Poland, www.piafproject.eu; 24 April 2012.
Wright David, De Hert Paul, editors. Privacy impact assessment. Dordrecht: Springer; 2012.
Wright David, Friedewald Michael, Gutwirth Serge, Langheinrich Marc, Mordini Emilio, Bellanova Rocco, et al. Sorting out smart surveillance. Computer Law & Security Review July 2010;26(4):343–54, http://www.sciencedirect.com/science/journal/02673649.