Chapter 17
Surveillance: Extending the Limits of Privacy Impact Assessment

Charles Raab and David Wright

17.1 Introduction

Privacy impact assessment (PIA) can be used to investigate the impact upon privacy that surveillance, using new information and communications technologies (ICTs) or information systems, might have before these applications are fully developed and implemented. PIA requires that an organisation subject its plans to more or less rigorous screening through the lens of privacy or data protection, to identify weaknesses in the innovation's compliance with relevant laws or principles, and to indicate how these might be eliminated. Myriad stakeholders potentially affected by the innovation may also be involved in this investigation. In an extreme situation, a project could be abandoned if its PIA indicated irremediable shortcomings.

As other chapters in this book show, a variety of PIA models exist across the world, in terms of their scope, procedures, the involvement of bodies such as regulatory agencies or civil society organisations, and transparency requirements. Some focus on information privacy (data protection) only, while others say that PIAs should address all types of privacy. PIA differs from privacy audits and other inspections and analyses of organisational data processing in that the latter are usually performed on systems and technologies already in use. As a fairly recent addition to the array of tools and methodologies that can be used to avoid or mitigate the negative impacts upon privacy of a new technology or service, PIA is required in some countries and strongly urged upon data collectors in others. Handbooks, guidance materials and examples of PIA are readily available.[1] PIA plays a part in an organisation's procedures for compliance with privacy and data protection laws and good

[1] For a compendium and analysis of PIA methodologies from seven countries and of 10 PIA reports, see Wright, David, et al. (eds.), *A Privacy Impact Assessment Framework (PIAF) Deliverable D1*, a report of the PIAF consortium prepared for the European Commission, September 2011. www.piafproject.eu

C. Raab (✉)
University of Edinburgh, Edinburgh EH8 9LD, Scotland
e-mail: c.d.raab@ed.ac.uk

D. Wright, P. De Hert (eds.), *Privacy Impact Assessment*, Law, Governance and Technology Series 6, DOI 10.1007/978-94-007-2543-0_17,

practice. These important contributions to privacy protection are likely to spread further in future, and PIA – especially if legally mandated to be carried out – may become one of the key instruments available to privacy policy-makers, regulators and practitioners themselves.

On the other hand, PIA is subject to a number of objections and limitations. This chapter briefly reviews them and offers some rebuttals before looking more closely at surveillance practices and their users: the what and who of surveillance. It then indicates some analytical dimensions of surveillance – their visibility, legality, power implications and targets – that raise ethical concerns. Following that, it reflects upon one of the main limitations of PIA: its nearly exclusive focus on privacy, to the neglect of a range of other individual and societal values, rights or freedoms that may be impacted by surveillance. In the light of this, the chapter finally considers how PIA could be extended to assess the impact of surveillance on this broader range.

17.2 Objections to Subjecting Surveillance to PIA

Sceptics and critics have often resisted the application of PIA techniques to surveillance projects on a variety of grounds. This section considers and rebuts some of these arguments.

17.2.1 A Brake on Technical Progress

Information and communication technologies – although themselves shaped by social processes – are among the most powerful drivers of today's economy and society. An argument can be mounted that the pace of technological development ought not to be slackened by the "interference" that PIA might represent, and that any adverse effects can be controlled by appropriate responses and resilience rather than through *ex ante*, or precautionary, application of PIA. This argument seems to prevail in the training and education of technologists as well as in the philosophy of those who use their products, so that special effort has been required in very recent years to insinuate the merits of PIA and "privacy by design" into the thinking and practice of the laboratory and boardroom.

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. Simply because there are precedents for this is no reason for sealing the issues off from deliberation and action that might reconfigure the relationship between technology and society. PIA takes its place alongside other techniques associated with technology assessment in seeking a different point of departure.

17.2.2 Some Surveillance Involves Central Functions of the State

It is often argued that the maintenance of public order, the enforcement of law and national security should exempt information activities from restrictions applied to systems that do not perform these functions, or that are in the private sector. It is held that the intensive and extensive use of personal data, video surveillance, interception of communications and biometric devices must be regarded as legitimate means to the paramount end of keeping us safe. Data protection law already provides exceptions from certain provisions and requirements where the prevention and detection of crime, and the safety of the state are at stake in the activities of certain organisations.[2] Therefore, it would inhibit the efficiency and effectiveness of the performance of these functions if the technologies and information systems involved in their pursuit had to be subject to privacy impact and other forms of assessment, and if their use would be limited or proscribed unless they met the recommendations exhorted in these assessments. Moreover, exposing details of surveillance systems to the public for scrutiny would damage the operations in which their use is intended. Overall, much of the argument is that, because these functions of the state are essential to the national or public interest, they therefore trump the individual interest in, or right to, privacy.

This is a powerful argument, especially in the climate of terrorist threat and public fears of disorder and crime. It would be a brave or foolish politician who would set her face against this mood and the realities of national security and law enforcement that accompany it. Revelation of technical details and operations in a PIA might indeed have adverse consequences for legitimate surveillance; this point is discussed further below, as a variant of it also applies in the commercial environment. On the other hand, the rule of law, the living legacy of human rights, and the workings of the system of justice are equally central to the national interest. Even the US Department of Homeland Security has recognised this, saying: "A PIA should be conducted for *all* systems handling personally identifiable information *including classified or law enforcement sensitive programs*."[3] [Italics added.] Where surveillance breaches the boundaries of necessity and proportionality, it must be subjected to checks whether anticipatory or remedial. Moreover, systems should be put in place – including PIA – to help determine whether a particular technological or information-management system is, in fact, necessary and not excessive if the objective is to be reached. While the hoary mottoes, "you can never be too safe" or "better safe than sorry", are poor guides to policy and practice where privacy and

[2] Until the Lisbon Treaty came into force in December 2009, the EU Data Protection Directive (95/46/EC) exempted second and third pillar issues from data protection scrutiny. The Lisbon Treaty now makes such scrutiny possible. With the planned revision of the Data Protection Directive, data controllers processing sensitive data, including surveillance systems, may be obliged to subject them to PIA.

[3] 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

other crucial values are threatened by surveillance, PIA – a technique rooted in risk analysis and discourse – could open up the question "how much safety do we need?" to serious scrutiny in specific instances.

If the security concerns are truly serious, these could be addressed by conducting a PIA with a non-disclosure agreement so that a representative group of stakeholders could be engaged in the process of evaluating the impacts on privacy of new security proposals. Furthermore, budget submissions for new security initiatives could be accompanied by a PIA 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 be sent to the Office of the Privacy Commissioner of Canada.[4] The funding agency could be given the power to turn down a budgetary submission if it judged the PIA to be inadequate; the Treasury Board in Canada has such a power. Post-PIA audits carried out by an independent third party could ensure the PIA recommendations were actually implemented. Such measures could be put in place to ensure that new security initiatives were subjected to a PIA without actually compromising security.

17.2.3 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 PIA. A PIA may violate security, the commercially sensitive nature of certain technical information, or the business case for an innovation, and exposure to external participants in the PIA process should therefore be avoided. Against this is the argument that ways can still be found to protect what needs to be protected for commercial or security reasons while still allowing the aims of a PIA to be achieved satisfactorily, including the transparency that publication of the PIA would ensure. In the United Kingdom, the Information Commissioner's Office (ICO) advises that sensitive details can be placed in a less widely distributed appendix and protected by confidentiality constraints, but counsels that such suppression should be limited to what can be justified, and that the concealment of poor thinking at the design stage could damage stakeholders' trust.[5] Maintaining or increasing public confidence in the legitimacy of properly regulated surveillance is, after all, an important objective of PIA. In any event, PIA is being taken up by the private sector: see the chapters in this book on Nokia, Siemens and Vodafone.

---

[4] "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", 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

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

The International Organization for Standardization (ISO) has developed a PIA for financial institutions (see Chapter 14), and an industry-developed PIA framework for radio frequency identification (RFID) has been endorsed by the Article 29 Data Protection Working Party (see Chapters 15 and 16). In Australia, the revised PIA guide has been developed to be applicable to the private sector[6] and the European Commission may oblige data controllers (including those in the private sector) who process sensitive data to carry out a PIA.[7]

17.2.4 Some Surveillance Involves More Than One Country

A further argument resisting PIA in circumstances of sensitive and secure operations is that the flow of personal data involved in the surveillance and information systems often takes place across national boundaries and is likely to involve objectives related to law enforcement and counter-terrorism, this time in an international or global setting. It could be claimed that the nature of these operations should rule out exposing their privacy and other impacts: the "trump card" justification, but with potentially more at stake than in many merely domestic environments. Moreover, conducting a PIA would seem to be somewhat difficult in procedural and organisational terms, as well as with regard to the applicable law with which the innovation should comply. This argument might seem difficult to rebut. However, although conducting a transnational PIA might be problematic, the countries involved in an international surveillance operation could nevertheless conduct their own PIA and, following its recommendations, negotiate with the other countries as necessary to ensure the surveillance operation was proportionate and necessary or to determine whether certain measures should 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.[8]

---

[6] Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, 2006, revised May 2010. http://www.privacy.gov.au.

[7] European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final, Brussels, 4.11.2010. http://ec.europa.eu/justice/news/intro/news_intro_en.htm#20101104

[8] 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.

The message here is that transnational projects should not escape the scrutiny of a PIA, simply because they are transnational. Even if government agencies have not yet put this in hand, transnational PIA has attracted some attention in the corporate world. The international consultancy Deloitte & Touche published a guide to cross-border privacy impact assessment as long ago as 2001,[9] although aimed at companies with cross-border operations rather than government agencies. More recently, a PIA has been performed for a transnational medical information project in Europe.[10] Robin Bayley and Colin Bennett (Chapter 7) refer to a PIA of a biometrics field trial involving the Canadian Citizenship and Immigration department, the US Immigration and Naturalization Service and the US Department of State.

17.2.5 Ineffectiveness Would Be Revealed by a PIA

Officials may not want to subject surveillance projects to a PIA lest system effectiveness be questioned in damaging ways, especially where the system is likely to be very costly. Politicians and the public, not to mention the suppliers of equipment and owners of premises, may have set great store by the supposed ability of a surveillance technology to achieve popular objectives. In the UK, closed-circuit television (CCTV) has been the single most heavily funded crime prevention measure operating outside the criminal justice system. The Home Office funded two major independent studies that cast serious doubt upon the effectiveness of CCTV, which had not produced the expected benefits, although improved performance might result from proper management and design.[11] The police themselves have questioned the utility of CCTV, and the Home Office and the Association of Chief Police Officers outlined a new CCTV strategy in 2007.[12] Although a PIA is not a retrospective audit, and conducting one for a changed system would aim primarily at assessing the impact on privacy and other values rather than functional effectiveness, it might also help to avoid such mistakes in future through the information that would be gathered and analysed about how the system works. With hindsight, if a PIA had been conducted from the inception of the British "love affair" with CCTV

---

[9] Karol, Thomas J., *A Guide To Cross-Border Privacy Impact Assessments*, Deloitte & Touche, 2001. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/A-Guide-To-Cross-Border-Privacy-Impact-Assessments.aspx

[10] Di Iorio, C.T., F. Carinci, J. Azzopardi et al., "Privacy Impact Assessment in the Design of Transnational Public Health Information Systems: The BIRO Project", *Journal of Medical Ethics*, Vol. 35, 2009, pp. 753–761. http://jme.bmj.com/content/35/12/753.abstract

[11] 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, pp. 120–121.

[12] Gerrard, Graeme, Garry Parkins, Ian Cunningham et al., National CCTV Strategy, Home Office and Association of Chief Police Officers, London, October 2007. http://www.bhphousing.co.uk/streetcare2.nsf/Files/LBBA-24/$FILE/Home%20Office%20National%20CCTV%20Strategy.pdf

that is carried on by local authorities, central government, the media and the general public, it might have had beneficial effects on performance as well as minimising the impact on privacy and legitimate social behaviour in public places.

17.2.6 PIA Is Too Narrowly Focused

This is a further objection, which is taken up at a later point. It is not that PIA is irrelevant, but that its scope in regard to surveillance currently is too limited because it mainly concerns impacts on individual privacy, not other rights and values. Therefore, it is unlikely to address the significance of surveillance for society as well as for individuals' lives and behaviour more broadly conceived, or to regulate its impact. This objection is rarely heard, but is important if the impact of surveillance is to be more fully assessed. This chapter builds on this objection in arguing that the range of impacts or risks to be considered should be extended. Before that point in the argument is reached, it is important to review various types of surveillance as well as the kinds of actors who engage in surveillance practices and the purposes served.

17.3 Types of Surveillance

With the development of new technologies, surveillance has become a much more complex set of processes than the literal meaning – to watch over – suggests. The many types of surveillance include watching, listening, locating, detecting and personal data monitoring[13] (or *dataveillance*, in Clarke's coinage[14]). In this section, we briefly describe the variety of surveillance types, some of which overlap, and then identify the main purposes and functions of these applications as well as the variety of surveillance users or "surveillants". The distinction between well-tried operational systems and those still undergoing development is important in describing examples of surveillance. So, too, is the distinction between ICTs that perform their intended and more or less discrete functions and those that have "crept" to new functions where regulatory understandings and rules, and social and individual impacts, may be less clear.

---

[13] For a more detailed discussion, see Ball, Kirstie, David Lyon, David Murakami Wood, Clive Norris and Charles Raab, *A Report on the Surveillance Society*, for the Information Commissioner by the Surveillance Studies Network (SSN), September 2006. http://ico.crl.uk.com/files/Surveillance%20society%20full%20report%20final.pdf. Raab, Charles, Kirstie Ball, Steve Graham, David Lyon, David Murakami Wood and Clive Norris, *The Surveillance Society – An Update Report on Developments Since the 2006 Report on the Surveillance Society*, Information Commissioner's Office, Wilmslow, Cheshire, November 2010. http://www.ico.gov.uk/news/current_topics.aspx. Monahan, Torin (ed.), *Surveillance and Security: Technological Politics and Power in Everyday Life*, Routledge, New York, 2006.

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

17.3.1 Watching

The visual connotation of surveillance is probably the most prominent one recognised by the public today. Visual surveillance is practised in public spaces and in private premises such as shops and office buildings, but this is not the place to ponder the legal or cultural distinction between "public" and "private". In many countries – perhaps especially the United Kingdom – the CCTV camera "stands for" surveillance. CCTV is used for automatic number-plate recognition (ANPR) – in some cases, also recording passengers' facial images – as well as for recognising suspicious or "abnormal" behaviour. It has been reported that software called Intelligence Pedestrian Surveillance "analyses clusters and movements of pixels in CCTV footage in search of 'behavioural oddities'", and that gait-recognition facilities are being developed. There are developments of intelligent software and a theoretical model to detect deviations from pre-defined "normal" patterns of behaviour,[15] as well as technologies that can "see" through clothing but supposedly not show anatomical details.[16] Small spy drones watch crowds at public events and are likely to play an important role in future, perhaps along with recognition technologies, for identifying individuals.[17]

17.3.2 Listening

Surveillance by eavesdropping or wiretapping (and wireless-tapping) – with or without judicial authorisation – usually targets individuals rather than groups. These practices have become much more difficult now that calls are packet-switched, when millions of people use Voice over Internet Protocol (VoIP), and when more calls than ever are encrypted. Watching and listening may merge in certain ICT applications: some scientists are developing artificial intelligence technology to enable CCTV cameras to "hear" sounds that suggest a crime is taking place and to capture it on film.[18]

17.3.3 Locating

Location tracking is being built into many products and services, including social networking, mobile telephony, control of convicted criminals or wayward school

[15] *ScienceDaily*, "Intelligent Surveillance System to Detect Aberrant Behavior by Drivers and Pedestrians", 21 Sept 2009. http://www.sciencedaily.com/releases/2009/09/090918100010.htm

[16] Leake, Jonathan, "Strip Search: Camera That Sees Through Clothes from 80ft Away", *The Sunday Times*, 9 Mar 2008. http://www.timesonline.co.uk/tol/news/uk/science/article3512019.ece

[17] Randerson, James, "Eye in the Sky: Police Use Drone to Spy on V Festival", *The Guardian*, 21Aug 2007. http://www.guardian.co.uk/uk_news/story/0,,2152983,00.html

[18] Williams, Rachel, "CCTV Cameras to be Given 'Ears'", *The Guardian*, 24 June 2008. http://www.guardian.co.uk/uk/2008/jun/24/ukcrime1

pupils, and vehicle safety systems, often anonymously but sometimes with discriminatory effects.[19] The European Data Protection Supervisor has cautioned that the technology for vehicle tracking would have "great impact on rights to privacy and data".[20]

Smart phones allow users to "geotag" images, indicating where and when the photo was taken, and then to upload them to their own websites or to those of social networks such as Facebook. Social networking through mobile phones or other devices can enable movable locations to be mutually known – a form of "participatory surveillance". Apple has built into its terms and conditions, and its privacy policy, a provision allowing the tracking of the user's precise location "anonymously in a form that does not personally identify" the user.[21]

17.3.4 Detecting

Some forms of surveillance involve detection by means of various technologies. These include those of ubiquitous computing or ambient intelligence, e.g., networking sensors and actuators, sometimes referred to as "smart dust", and RFID devices. RFID's many uses include machine-readable passports, identity cards, loyalty cards and travel cards.[22]

Other technologies – still experimental – can detect "abnormal" behaviour of suspicious characters, for example, passing through airports, by scrutinising pulse and breathing rates, and fleeting "micro-expressions".[23] Terrorists are often trained

---

[19] See Phillips, David, and Michael Curry, "Privacy and the Phenetic Urge: Geodemographics and the Changing Spatiality of Local Practice", in David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination,* Routledge, London, 2003.

[20] Lewis, Paul, "Big Brother Is Watching: Surveillance Box to Track Drivers is Backed", *The Guardian*, 31 March 2009. http://www.guardian.co.uk/uk/2009/mar/31/surveillance-transport-communication-box. See also Bennett, Colin, Charles Raab and Priscilla Regan, "People and Place: Patterns of Individual Identification within Intelligent Transportation Systems", in Lyon, 2003, op. cit., fn. 18.

[21] Quoted in Myslewski, Rik, "Apple Tweaks Privacy Policy to Juice Location Tracking", *The Register*, 22 June 2010. http://www.theregister.co.uk/2010/06/22/apple_location_terms_and_conditions/.

[22] For more on RFID applications and their implications, see, for example, OECD, *RFID Guidance and Reports*, OECD Digital Economy Papers, No. 150, OECD publishing, Paris, 2008; van Lieshout, Marc, Luigi Grossi, Graziella Spinelli et al., *RFID Technologies: Emerging Issues, Challenges and Policy Options*, European Commission, Joint Research Centre, Institute for Prospective Technological Studies, Office for Official Publications of the European Communities, Luxembourg, 2007; Ontario Information and Privacy Commissioner, *Privacy Guidelines for RFID Information Systems*, June 2006.

[23] Marks, Paul, "'Pre-crime' Detector Shows Promise", *New Scientist*, 23 September 2008. http://www.newscientist.com/blogs/shortsharpscience/2008/09/precrime-detector-is-showing-p.html. See also *The Economist*, "Surveillance Technology: If Looks Could Kill", 23 Oct 2008. http://www.economist.com/science/displaystory.cfm?story_id=12465303; and Sample, Ian, "Security Firms Working on Devices to Spot Would-Be Terrorists in Crowd", *The Guardian*, 9 Aug 2007. http://www.guardian.co.uk/science/2007/aug/09/terrorism

to conceal emotions; micro-expressions, however, are largely involuntary and are accentuated by deliberate attempts to suppress facial expressions. Research has been conducted into compiling physiological data, correlated with data on the subject's emotional and mental state to identify people intent on committing serious crimes.[24]

17.3.5 Dataveillance

Dataveillance involves activities that use collections of personal data – databases – in extensive and intensive ways for many purposes. It is a defining characteristic of the modern bureaucratic state, and of huge swathes of the modern economy. An array of dataveillance applications, including data monitoring, sharing, aggregation and mining, are used in the provision of public services and in marketing. Online monitoring of what people download or of which websites they visit is also a form of dataveillance. So, too, is the retention and analysis of electronic records of telephone calls and Internet usage for law-enforcement and counter-terrorism purposes, as in the European Union's (EU) Data Retention Directive 2006/24/EC. The Directive's financial and civil liberties implications have generated controversy.[25]

Another controversial instance of dataveillance concerns the monitoring of financial transactions to spot transfers made by criminals and terrorists through the Brussels-based Society for Worldwide Interbank Financial Telecommunication (SWIFT) system, thus allowing the CIA, the FBI and other agencies to examine large numbers of transactions.[26] Dataveillance is involved when governments and firms attempt to counter piracy on the Internet. Dataveillance also uses international travel data that are recorded and stored on government databases for many years in order to tighten border controls and fight terrorist threats. But among the main uses of extensive dataveillance are those in the operations of states and companies carrying out myriad everyday dealings with citizens or customers. The drive for joined-up service provision and for efficient marketing, especially online, has placed a premium on the collection and processing of large quantities of detailed personal data in the "database state".

17.3.6 Assemblages

Stand-alone surveillance technologies or systems can be combined into "assemblages": for example, digital CCTV combined with facial recognition or

[24] See, for example, *The Washington Post*, "Gallery: Anti-deception Technologies", 18 July 2010. http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/

[25] Article 29 Data Protection Working Party, "European Data Protection Authorities find Current Implementation of Data Retention Directive Unlawful", Press release, Brussels, 14 July 2010. http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

[26] Lichtblau, Eric, and James Risen, "Bank Data Is Sifted by U.S. in Secret to Block Terror", *The New York Times*, 23 June 2006.

video content analysis. Smart CCTV has developed software that analyses the movements of people or vehicles; the CCTV operator checks the image and, if concerned, rings the police. Other possible uses of algorithmic systems concern the detection of suspicious behaviour and packages on public transport.

Assemblages can also involve the pooling or aggregation of data. The accuracy of assemblage technologies can be doubted, for there may be many false positives flagging up innocent people as suspicious. This inaccuracy, as shown in technical trials, is one reason why the UK government has moved away from "voice-risk analysis" of eavesdropped telephone calls to catch "benefit cheats".[27]

17.3.7 Surveillance: Causes of Concern

In sum, the technologies and applications of surveillance are legion, and many more examples could be given of their variety and combination.[28] Suffice it to say that surveillance throws up many causes of concern about its effect on persons, groups and society, and that impact assessment – in the form of PIA – is a valuable instrument for mitigation. At this point, it is relevant to identify three causes of concern about surveillance that are important in analysis and in considering regulatory measures.

The first is its *visibility*: surveillance can be visible or invisible from both a technological and a human point of view. Some surveillance is invisible because the surveillants do not want a target to know of the surveillance; for example, where law enforcement authorities intercept a suspect's communications or where a company bugs politicians.[29] The second is *legality*: it is not always apparent whether a particular surveillance practice is legal or not. The grounds for legality vary across jurisdictions. Some practices may be declared illegal if, for example, their operators have failed to get the necessary warrants, perhaps especially if the surveillance is covert, such as in planting a global positioning system (GPS) device in a suspect's car.[30] Some practices may be thought to be of dubious legality, leading to legal challenges as to their proportionality, necessity or compatibility with the target's "reasonable expectation of privacy".

The third is the *power implications* of surveillance. Surveillance implies a power relationship between the surveillants and the surveilled, where the latter is at a power disadvantage to the former, resulting in other adversities flowing from the

---

[27] Sample, Ian, "Government Abandons Lie Detector Tests for Catching Benefit Cheats", *The Guardian*, 9 November 2010. http://www.guardian.co.uk/science/2010/nov/09/lie-detector-tests-benefit-cheats

[28] See Ball, Lyon et al., op. cit., fn. 12, and Raab, Ball et al., op. cit., fn. 12.

[29] Goslett, Miles, "Your Office May Have Been Bugged by BAE, Investigators Told MP", *Daily Mail*, 3 Oct 2009. http://www.dailymail.co.uk/news/article-1217919/Your-office-bugged-BAE-investigators-told-MP.html.

[30] *The New York Times*, "GPS and Privacy Rights", Editorial, 14 May 2009. http://www.nytimes.com/2009/05/15/opinion/15fri3.html

surveillance itself. However, the relationships between surveillants and surveilled are much more complex and nuanced. Power implications will be particularly relevant to the later discussion about surveillance impact assessment.

17.4 Who Are the Surveillants, and Why Do They Use Surveillance?

With reference to the types of surveillance reviewed above, the ubiquity of technologies and the influence of complex motivations mean that there is a large variety of surveillants, in both the public and private sectors. In the following paragraphs, we identify three main groups of surveillants and their major purposes. Many surveillants use all types of surveillance to target specific individuals and groups, while others use a narrower range depending on the means available, the purpose and the desired target. It is not a question of what "they" are doing to "us": with the willingness of so many people to put so much personal data on social networks, some experts have described the phenomenon as "participatory surveillance":[31] the witting or unwitting involvement of the surveilled in surveillance practices. It should also be borne in mind that – beyond the intended purposes – surveillance involves many unintended side-effects that would need close examination in an application of PIA.

17.4.1 Public Sector

Governments conduct surveillance for many purposes. These range from security, policing, checking benefits entitlement and preventing fraud or (at the local level) detecting misdemeanours, charging vehicles in traffic-congested inner cities, checking up on dubious school catchment-area residents or catching owners whose dogs foul the pavement. Intelligence and law-enforcement agencies typically use surveillance of electronic communications, often with the support of telecom carriers and ISPs. Covert surveillance is frequent: police forces usually argue that this is necessary to investigate paedophiles, Internet fraudsters, identity thieves, terrorists and other "cybercrime" suspects. Surveillance, and particularly information practices associated with dataveillance in the widest sense, is often used by the "welfare" parts of the state, and in health and care services, to underpin a variety of precautionary or responsive practices aimed at people in need or at risk. Thus, surveillance is used in the public sector, and at all levels of the state from local to central – and indeed, beyond state borders – for purposes of sanctioning as well as benefitting

[31] "Online social networking seems to introduce a participatory approach to surveillance, which can empower – and not necessarily violate – the user." Albrechtslund, Anders, "Online Social Networking as Participatory Surveillance", *First Monday*, Vol. 13, No. 3, 3 March 2008. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2142/1949

the general public or sections of the population. Different government agencies may also share the data they amass.[32] Some surveillants may operate either in the public or the private sector. In controlling the behaviour of pupils, students or visitors, education institutions use CCTV as a precautionary or investigatory tool for purposes of maintaining order or fighting crime. They also use biometric devices to control entry and exit to premises, and in schools' catering and library facilities. Managers of hospitals, airports, rail stations and networks, and other infrastructure or service facilities use surveillance to prevent and detect not only malfunctions and criminal behaviour, but also disruptive or malicious attacks such as may be involved in terrorist activity. Surveillance thus plays an important role in the protection of critical infrastructures, whether public or private.

17.4.2 Private Sector

Companies' commercial purposes have been highlighted in the discussion of types of surveillance. Profiling of customers through the intensive analysis of information plays a central part in modern marketing. ISPs and search engines have tracked users' surfing habits by a variety of means, including cookies, giving an important business capability and, in particular, selling advertising space. Receivers installed around a shopping centre or trade show allow a company to pick up communication between individuals' mobile phones and base stations, and thereby track visits and re-visits to exhibits or shops, and how long a visitor spends in each. Journalists have engaged in sometimes illegal surveillance and interception of telephone calls, for example, in pursuit of "investigative" stories concerning celebrities.[33] Surveillance of employees has long been controversial, pitting employee privacy against employer interests in ensuring employees are doing what they are paid to do, and not misusing company facilities such as e-mail and the Internet.

17.4.3 Society

Surveillance is widespread in society, used by a wide variety of people. Major examples include those intending to carry out criminal or terrorist acts: burglars, for example, may use Web-based surveillance techniques to monitor the whereabouts of targeted individuals or activity in their households. Stalkers and extortionists can insert a Trojan or other virus on users' computers. Others engage in corporate espionage for business, national or military advantage. In today's safety-oriented

[32] Thomas, Richard, and Mark Walport, *Data Sharing Review Report*, 11 July 2008. www.justice.gov.uk/docs/data-sharing-review-report.pdf

[33] Davoudi, Salamander, "Newspaper Phone-Hacking Scandal Widens", *The Financial Times*, 14 Mar 2011. http://www.ft.com/cms/s/0/4dbe102c-4e28-11e0-a9fa-00144feab49a.html#axzz1Gdl4ObsB

culture, parents may track their children as the latter travel to and from school or around the world. Surveillance may be endemic because many people are naturally suspicious: survey evidence has shown the extent to which, among married couples, spouses snoop on each other's e-mails, text messages and patterns of Internet use.[34] In addition, the recreational or entertainment use of surveillance cannot be discounted. Surveillance of others is "fun" for some people, as the popularity of social networking and reality TV suggests; surveillance powerfully shapes, if not defines, our culture. This indicates a shortcoming of PIA: while it can be applied to many types of surveillants in the public and private sectors, surveillance used more generally and amorphously in society cannot be subjected to its rigours; other regulatory instruments, including the application of the law, are more appropriate – even if they are weak in the circumstances of societal surveillants as well as in the global flow of personal information.

17.5 Assessing Surveillance Effects: Privacy and Beyond

PIA presupposes a perspective on some dimensions of privacy that might be affected by surveillance; this section explores some considerations on that issue. It then moves towards a new way of thinking about PIA by placing it in the innermost of several concentric circles of impact analysis of surveillance and describing the wider dimensions that might be affected, and that should therefore be taken into account. This yields a suite of PIAs ranging from PIA_1 to PIA_4. For analytical purposes, this formulation refines and differentiates the approach taken in a prominent report on surveillance, in which "surveillance impact assessment" (SIA) was seen as a development of PIA in the direction of recognising wider impacts, but it amends the terminology.[35] "Impact Assessment" (IA) is the root of these evaluations; the prefix "privacy" in conventional PIA suggests that the impact under consideration is the privacy of the individual, but this is not so straightforward. Although, in the EU, privacy is seen as both a fundamental right and a societal value, there is no universally agreed definition of privacy, and diverse ways in which privacy can be understood.

Privacy has been defined in different ways, but a widely agreed definition remains elusive. It is a difficult term to define because it means different things to different people in different contexts at different times. Many privacy scholars have commented on the difficulty of defining privacy. James Whitman, for example, has observed that "privacy, fundamentally important though it may be, is an unusually slippery concept. In particular, the sense of what must be kept 'private,' of what

[34] The survey was part of a larger project. See Oxford Internet Institute, "Me, My Spouse and the Internet: Meeting, Dating and Marriage in the Digital Age", January 2008. http://www.oii.ox.ac.uk/research/projects/?id=47.

[35] Ball, Lyon et al., op. cit., fn. 11, p. 93. "Surveillance impact assessment" is a misleading term if – paralleling the meaning of PIA as the assessment of impact on privacy – it is construed as the assessment of impacts on surveillance, which would be meaningless.

must be hidden before the eyes of others, seems to differ strangely from society to society." The "slipperiness" of privacy is compounded by virtue of the fact that the "ideas of privacy have shifted and mutated over time".[36] To cite another example, Daniel Solove describes privacy as "a concept in disarray. . . . Currently, privacy is a sweeping concept, encompassing (among other things), freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations."[37] Solove therefore eschews any search for a single definition, essence or common denominator and adopts a Wittgensteinian approach, seeing "family resemblances" in the plurality of contexts in which privacy *problems* are said to arise, so that privacy becomes an "umbrella term".[38] In this perspective, context becomes an important key to understanding and protecting privacy, as Helen Nissenbaum's analysis shows.[39]

A pluralistic approach is useful in that it allows the retention of "privacy" as a general prefix to IA while enabling distinctions between the different kinds and extents of impact that different kinds of surveillance may bring about. PIA_1, $_2$, $_3$ and $_4$ therefore map onto these various meanings and associations within privacy's conceptual family, resembling but framing differently, the useful delineation of types of privacy found in other writing. For example, corresponding to well-grounded approaches to understanding privacy, the ICO usefully identifies four conventional but overlapping dimensions of privacy: privacy of personal information, privacy of the person, privacy of personal behaviour and privacy of personal communications.[40] Privacy can be taken to have intrinsic worth, connected with ideas of dignity, autonomy and a sense of being a person. Privacy involves being "let alone", being forgotten when desired or where desirable, and being able to exert some control over one's personal information. Privacy can also be justified on more instrumental or utilitarian grounds. Without it, individuals would find it difficult to develop their personalities, engage in social relationships, separate their personal and public lives, or enjoy important freedoms, including freedom of religion, freedom of expression and freedom of association.[41]

---

[36] Whitman, James Q., "The Two Western Cultures of Privacy: Dignity Versus Liberty", *The Yale Law Journal*, Vol. 113, 2004, pp. 1151–1221 [pp. 1153–1154].

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

[38] Solove, ibid., ch.3.

[39] Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, CA, 2010. See also her earlier paper: "Privacy as Contextual Integrity", *Washington Law Review*, Vol. 79, No. 1, 2004, pp. 101–139. http://www.nyu.edu/projects/nissenbaum/main_cv.html

[40] ICO, PIA *Handbook*, p. 14. These four types of privacy draw on Roger Clarke's categorisations. See Clarke, Roger, "What's Privacy?", 2006. http://www.rogerclarke.com/DV/Privacy.html

[41] For a range of writings across the spectrum of meanings, see Schoeman, Ferdinand D. (ed.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, Cambridge, UK, 1984.

These other utilities, rights and freedoms are reflected in the further circles identified below because they embody values that are vital to individuals, but also have important implications for others, and for society. They tap the dimension of *sociality* in individual behaviour as well as the dimension of the public interest in mitigating the impacts of surveillance for the sake of preserving the values of society and the political system. An increasing number of scholars have pointed to the social value of privacy. Priscilla Regan was one of the first to develop an argument showing its importance to society, commenting that

> Privacy has value beyond its usefulness in helping the individual maintain his or her dignity or develop personal relationships. Most privacy scholars emphasize that the individual is better off if privacy exists; I argue that society is better off as well when privacy exists. I maintain that privacy serves not just individual interests but also common, public, and collective purposes. If privacy becomes less important to one individual in one particular context, or even to several individuals in several contexts, it would still be important as a value because it serves other crucial functions beyond those that it performs for a particular individual.[42]

The range of surveillance forms described earlier can be seen as affecting privacy in one or more of these connotations of the term. It is hard to find ways to be let alone if one is subjected to listening and watching, tracking and detecting. It is not easy to maintain a sense of personal dignity when faced with body scanning, fingerprinting and electronic tagging. Autonomy is affected by behavioural monitoring and database profiling, and the sense that one is able to associate freely with others – socially and politically – is reduced by video surveillance, eavesdropping on communications and long-term retention and sharing of information by organisations. These and other effects may be the more insidious to the extent that surveillance is covert, or thought to be taking place without knowing when, how or why.

For all its admirable qualities, PIA tends only to concern surveillance's impact on individual privacy, not on other rights and values pertaining to the individual or its impact on other targets and entities, intended or not. These other impacts are not normally recognised in the risk analysis that PIA prescribes. As was mentioned earlier, this can be seen as an objection to conducting a PIA, albeit in the sense that a PIA is necessary but insufficient to address all of the impacts that surveillance may have. Surveillance scholars plausibly argue that privacy incursion is not the main concern to highlight in evaluating the effects of watching, detecting, data-mining and other surveillance techniques. It would follow that PIA as conventionally conceived, while useful, leaves a great deal out of account – or out of accountability. This is not to deny the crucial importance of privacy to the individual, making its protection imperative as a human right. However, PIA tends mainly to assess the prospective compliance of new technologies or systems involved in surveillance

---

[42] Regan, Priscilla M., *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, Chapel Hill, 1995, p. 221. See also Raab, Charles, "Privacy, Social Values, and the Public Interest" and Rössler, Beate, "Soziale Dimensionen des Privaten", both in *Politische Vierteljahresschrift*, Special Issue 46 (2011) on "Politik und die Regulierung von Information".

with the canonical, though limited, inventory of "fair information" principles or practices pertaining to "personal data" – itself an ambiguous and controversial concept. These principles are enshrined, with variations, in every information privacy law and in international documents,[43] and are likely to persist through the likely revisions of these laws and instruments. Data protection principles are an essential bedrock, but they do not fully address the range of questions that should be asked about surveillance, especially the "new surveillance" brought about through new technologies and information systems.[44]

By focusing only, or mainly, on the privacy of the individual data subject, PIA has little directly to say about the effects of particular surveillance forms upon wider and cumulative circles of individual and civic values that may not necessarily be inherent in, or commonly understood as part of, the concept of privacy. Conventional PIA, therefore, constitutes the first, innermost circle, which can be called "PIA_1", but there are three further kinds of orientation for an IA that goes beyond PIA (see Fig. 17.1 and Table 17.1). The rest of the PIA suite would assess the form or technology in question against other meanings of privacy that take wider ranges of impact into serious consideration.

Impact assessment in the second, wider circle – called "PIA_2" – remains close to the realm of individual values and rights, but does not stop at considering the most conventionally understood privacy impacts. It takes into account the risk posed by surveillance to the individual's social and political relationships, and her relative position within society and the market, as the potentially impacted objects.

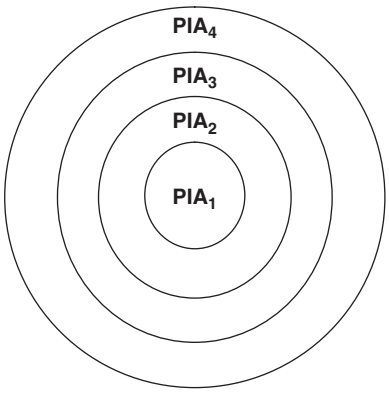

Fig. 17.1 Circles of PIA

[43] Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, The MIT Press, Cambridge, MA, 2006.

[44] 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. http://www.surveillance-and-society.org/journalv1i1.htm

Table 17.1 Extending the limits of PIA

PIA_1	PIA_2	PIA_3	PIA_4
Focuses on individual privacy	Focuses on PIA_1 + other impacts on individual's relationships, positions and freedoms	Focuses on PIA_2 + impacts on groups and categories	Focuses on PIA_3 + impacts on society and political system

Among them are also the individual's freedom of speech and association: political and social values that are enshrined as foundational in western-style liberal democracies and in conceptions of the nature of society and interpersonal relationships at several levels of scale. These freedoms might well be infringed by ICTs and information processing, as when video surveillance or electronic eavesdropping makes it risky for people to communicate with one another or to join associations whose activities are monitored closely. This is the much-discussed "chilling effect" of public-space surveillance or of communications monitoring upon sociability and legitimate political participation.

The third circle of IA – "PIA_3" – incorporates the first and second, but is also concerned with surveillance's effect on the groups and categories to which individuals belong, or to which their membership is attributed by others. Individual privacy may be affected by the way individuals are thought of, or are treated, as members of wider categories, classes or groups. How these trans-individual entities are administratively or socially constructed, or individually self-selected, is important in understanding the impact of surveillance, but is somewhat outside the scope of this chapter to explore in detail. However, PIA needs to take account of these broader reaches in terms of who might be affected. The ICO, for example, enumerates those whose safety is at risk if their personal data are disclosed: people who are under the direct threat of violence; celebrities, notorieties and VIPs; and people in security-sensitive roles. Then there are "vulnerable populations", including young children or adults who are incapable of providing consent, the homeless, ex-prisoners, refugees and those with certain health conditions.[45]

But this catalogue is too constrained: one might want prominently to add groups or categories identified by characteristics that include ethnicity, race, religion, national origin, political affiliation and sexual orientation, all of which might be the subject of surveillance techniques performed on these groups or categories as such, led by suspicions about the propensity of such persons to endanger the state or society. The profiling of individuals and social groups through the intensive analysis of digitised data in order to make decisions about their treatment by the state or the market provides another example of these effects. The principles of equality and non-discrimination could be negated by the profiling activities of commercial or state organisations. These employ techniques that target not only certain individuals, but also groups or categories of persons through an intensive analysis of collections

[45] ICO, PIA *Handbook*, p. 19.

of personal data. On the basis of the analysis, decisions or judgements are made about the role of individuals or groups and categories in the market, their potential to commit crimes, or their creditworthiness – and thus, colloquially, their moral character – that have consequences for their lives or well-being. Thus, beyond having a privacy impact as such, profiling and classification – possibly through obscure and opaque analytical processes – can affect the access to goods and services, and the power to act and participate as social beings, that may be experienced by individuals sharing a similar fate, and the adversity is compounded if the classification is erroneous or arbitrary.[46] The involvement of stakeholders in PIA, or in any other form of IA, is more likely to bring these matters to the surface if collectivities of individuals are recognised as having a stake in the implementation of surveillance technologies and systems.

Whether or not one is particularly concerned about the loss of one's own privacy, the reduction in society's ability to sustain privacy as a general good and a constitutive value has consequences for citizenship and the relation between the individual and the state or other organisations. Going even further than an assessment of impacts on privacy and a range of other individual or group values, on the outermost circle – "PIA_4" – the effects of surveillance on the workings of society and the political system as such would be assessed. This chapter falls short of elaborating such a wide-ranging "societal impact assessment" but is in sympathy with attempts to do so. This is because the social and political value of privacy is coming to be recognised as important, or – putting it another way – the effects of surveillance are felt in ways that go beyond the conventional paradigm of what "privacy" means, even taking into account the variety of traditional meanings as well as the distributive justice implicit in critiques of social sorting, to involve yet further values that recent authors emphasise.[47] These effects are felt in terms of what they portend for the texture of society and the constitutive properties of liberal, democratic political systems. Taken together, these trans-individual values form some of the most important fundamentals of these societies and polities. If surveillance through ICTs and information processing potentially affects the ability to realise these values, as well as individuals' ability to enjoy well-established rights, it would seem important to implement assessment techniques – including privacy but widening the focus to take in impacts beyond it – and to link them to remedial or preventive action to mitigate these effects. The effect of surveillance upon society and the polity, and not only on individuals as entities to whom rights pertain, is likely to be missed in the performance of PIA unless it is repositioned to assess the impact of surveillance in broad terms.

---

[46] See Lyon, David (ed.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, Routledge, London, 2003, and Vedder, Anton, *The Values of Freedom*, Aurelia Domus Artium, Utrecht, 1995, Chapter 4, re "categorial privacy". More generally on the consequences of classification, see Bowker, Geoffrey C., and Susan L. Star, *Sorting Things Out: Classification and Its Consequences*, MIT Press, Cambridge, MA, 1999.

[47] See Regan, 1995, op. cit., fn. 39, Chapter 8; Goold, Benjamin J., "Surveillance and the Political Value of Privacy", *Amsterdam Law Forum*, Vol. 1, No. 4, August 2009; Rössler, op. cit., fn. 42, and Raab, op. cit., fn. 42.

Of course, *what kind* and *how much* privacy and in what contexts it is important are endlessly debatable questions, but so too are what kind and how much surveillance and in what contexts. Not all of the effects on privacy occur to the same degree of severity, and different kinds of surveillance affect privacy differently, as a PIA would show. As indicated earlier, an understanding of contexts[48] is crucial if PIA is to result in usable recommendations for improving information systems and technologies, rather than in black-and-white judgements. Contexts mediate the effects – mitigating or amplifying them – and may enable individuals to influence the ways in which their privacy is, is not, or is less severely eroded by a particular surveillance technology operating in a particular place at a particular time. These nuances contribute powerfully to the lived experience of being under surveillance, and may arbitrate the need for more reliable safeguards to be built into information systems – one of the outcomes of PIA – or for more stringent control mechanisms found in the law and other instruments of regulation.

17.6 Conclusion

PIA by itself, on whatever circle, is not a silver bullet for privacy protection, but it can exert a strong influence on the culture, structure and behaviour of organisations that deploy surveillance. Maximising that influence depends on how securely PIA is embedded in organisational routines and in the information governance strategies adopted for the handling of personal data. That, in turn, may depend on internal and external leadership and on the requirements and sanctions that are brought to bear to improve privacy orientation and practice. PIA cannot engineer these components, but can contribute to making their necessity more palpable.

However, there are other shortcomings within PIA itself. One is the extent to which a particular form of PIA emphasises the importance of privacy rights and values as the rationale for the PIA approach and the solutions it recommends, rather than the risks to the organisation itself. Selling PIA to a government department or a commercial firm may require a business or policy case to be established as an inducement to undertake PIA, but the assessment will be caught short if the impression is given that PIA is about protecting the organisation's reputation, balance sheet or legality, more than about protecting the privacy of those affected by the information or surveillance system and practice that is being assessed. A PIA should address both aspects.

In the perspective of this chapter, however, the most important shortcoming would be the restriction of PIA largely to assessing the impact on individuals, even if its recognition that categories and groups might be at risk takes a step into the field of considering wider impacts, and ultimately impacts on society as a whole. As mentioned earlier, this recognition is more likely to be reinforced if the participation of stakeholders reflects and represents important segments of the population

[48] Nissenbaum, 2010, op cit., fn. 38. See also Solove, op. cit, fn. 36.

who may be especially affected by surveillance. The effects to be investigated by a PIA that goes one or more steps beyond the entry level of a PIA would include social exclusion and categorical discrimination, by which choices and life-chances for individuals and groups are limited beyond any incursion of privacy that surveillance may cause, thus adversely shaping the nature and texture of society. If taken into consideration, the criteria for assessment would bring PIA closer to ethical impact assessment, discussed in Chapter 19 in this volume. It would also underline the importance of privacy as a human right, seen not only in terms of its value for the individual alone, but for a society made up of privacy-protected individuals who are capable of, and empowered to, engage in a variety of social and political relationships at various levels of scale – or refrain from such engagement, if they choose – free of the restrictions imposed or implied by certain forms and degrees of surveillance.

Further afield, PIA_4 would address some of the most subtle and neglected dimensions of the discourse and practice of privacy invasion through surveillance: matters concerning society, the polity and the public interest broadly conceived. How this kind of assessment would be constructed is not only unfinished business, but has scarcely begun. Whether the analytical distinctions made in this chapter can be translated into practice is the proof of the pudding, but the ingredients themselves may nevertheless be of practical worth in developing ways of assessing the impact of new technologies and systems of surveillance.