Regulating Surveillance: Suggestions for a Possible Way Forward

Moira Paterson*

The need for privacy protection against surveillance has assumed new significance due to the onslaught of technological developments that increasingly undermine the capacity of individuals to maintain anonymity in relation to public activities and their physical movements across public places. Modern surveillance practices arguably require a rethinking of some of the tests and assumptions that underlie existing privacy laws, including tests based on "reasonable expectations of privacy", distinctions between content and between transactional data and content. They also call for active consideration of the full range of regulatory tools available and ways in which those tools can be adapted to reduce their existing limitations. This paper draws on a range of privacy resources, and on regulatory theory more generally, to suggest possible ways forward.

* Professor of Law, Monash University. Early drafts of this article were presented at the Privacy Law Scholars Conference at the George Washington School of Law on 6 June 2014 and at the Law & Technology Workshop at Tel Aviv University on 5 December 2016. I wish to record my thanks for the valuable feedback received at each of these events.

I. Introduction

The need for privacy protection against surveillance has assumed new significance due to the onslaught of technological developments that increasingly undermine the capacity of individuals to maintain anonymity in relation to public activities and their physical movements across public places. Two examples are illustrative of this trend.

The first is the FaceSDK application, which is advertised as enabling developers using a variety of computing languages to build platforms based on face recognition. This is described as being "used in hundreds of applications for identifying and authenticating users with webcams, looking up matching faces in photo databases, automatically detecting facial features in graphic editors, and detecting faces on still images and video streams in real-time".[1]

The second is a recently developed "IMSI catcher" device, which is described as "a low-cost way to discover the precise location of

1. See Luxand Inc, "Detect and Recognize Faces with Luxand FaceSDK" *Luxand*, online: Luxand <https://www.luxand.com/facesdk/>.

smartphones using the latest LTE standard[2] for mobile networks"[3] and as being able to "track users for days with little indication anything is amiss".[4]

What is significant about technologies of this type is that they make it increasingly easy to extract or infer identity from non-identifying signs and information. This amounts to an unprecedented assault on anonymity, making it increasingly difficult for individuals, other than hermits, to go about their lives beyond the reach of others. More specifically, these technologies make it difficult for individuals to keep at bay the uncalled for reactions and consequences that result from being known to and accessible by random and unknown individuals and entities who use the aforementioned devices and applications.

The implications of technology-assisted surveillance activities have, to date, been considered most closely in the context of surveillance by law enforcement and national security bodies. They have also received some scrutiny in the online context. However, it is arguable that there is also a need to regulate surveillance more generally, especially as it relates to public places.

Across the board surveillance is important because surveillance and the possible privacy harm to which it may give rise are no longer solely the main provinces of law enforcement and national security bodies; surveillance now underlies many of the decision-making processes of businesses in relation to current and prospective customers and employees, and it is increasingly within the reach of private individuals as discussed below. The regulation of surveillance more generally is also important because of the erosion of the boundaries between public

2. The Long Term Evaluation Standard is a 4G mobile communications standard for high-speed wireless communication for mobile phones and data terminal: See "LTE (telecommunication)" *Wikipedia* (11 November 2017), online: Wikipedia <https://en.wikipedia.org/wiki/LTE_(telecommunication)>.
3. Dan Goodin, "Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations" *Ars Technica* (28 October 2015), online: Ars Technica <arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/>.
4. *Ibid*.

and private surveillance. As made clear most recently by the revelations of Edward Snowden, private sector organisations are in many ways complicit in surveillance activities by national security organisations. This means that personal data collected within the private sector provides an additional pool of information for law enforcement and national security organisations to utilise.[5]

Modern surveillance practices arguably require a rethinking of some of the tests and assumptions that underlie existing privacy laws, including tests based on "reasonable expectations of privacy", distinctions between content, and between transactional data and content. They also call for active consideration of the full range of regulatory tools available and ways in which they can be adapted to reduce their existing limitations. This paper draws on a range of privacy resources, and on regulatory theory more generally, to suggest possible ways forward.

II. The Problem of Privacy in Public Places

Public place privacy has become a major issue due to technological developments that facilitate "round the clock" surveillance, evolving social practices that increase the amount of information disclosed by individuals about themselves and changes in the decision-making practices of businesses and government agencies involving information obtained via directed, ongoing surveillance as a basis for making decisions about individuals. These are increasingly combining to create what has been described as "seamless, real-time surveillance".[6]

The link between technology and issues of privacy is by no means

5. See *e.g.* Ewen MacAskill & Dominic Rushe "Snowden document reveals key role of companies in NSA data collection" *The Guardian* (1 November 2013), online: The Guardian <www.theguardian.com/world/2013/nov/01/nsa-data-collection-tech-firms>. This threat is arguably amplified to the extent that countries impose compulsory data retention regimes. For useful discussion of the Australian context see Dan Svantesson, "Systematic Government Access to Private-Sector Data in Australia" (2012) 2:4 International Data Privacy Law 268.
6. Edem Williams & Bassey Eyo, "Ubiquitous Computing: The Technology for Boundless Surveillance" (2012) 3:9 International Journal of Scientific & Engineering Research 1 at 2.

new. Early concerns about effects on privacy were highlighted by Warren and Brandeis back in 1890.[7] They related to "instantaneous photographs" and numerous mechanical devices that threatened to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops".[8]

The impact of technology accelerated in the latter part of the 20th century with the advent of digitisation and the convergence that it facilitated, as well as developments such as the increased use of loyalty cards and closed circuit television ("CCTV") cameras.[9] It has accelerated even further in the new millennium due, in particular, to three trends: (1) the proliferation of Radio Frequency Identification ("RFID") that facilitates comprehensive but unobtrusive 'round the clock' surveillance via its use, for example, on freeway transponders and public transport swipe cards; (2) the increased use of Global Positioning Systems ("GPS") to collect data about individuals' geographical locations across time, thereby creating detailed profiles not only of an individual's movements but also of their interrelationships with others; and (3) advances in imaging algorithms (for example, those used for face recognition and automatic number plate recognition), which facilitate the automated operation of CCTV networks and other visual surveillance activities.[10]

These technologies are converging and being combined to create powerful, networked surveillance systems that come close to realising Weiser's vision of a new era of ubiquitous computing ("ubicomp"). This ubicomp era is one in which computer technology would become embedded in all aspects of daily life and computing would increasingly "move to the background, weave itself into the fabric of everyday living

7. Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4:5 Harvard Law Review 193.
8. *Ibid* at 195.
9. For a useful overview of these and other early technology-related issues see Australian Law Reform Commission, *Review of Australian Privacy Law* (Discussion Paper No 72) (ALRC 2007) ch 6 (September 2007), online: ALRC <https://www.alrc.gov.au/sites/default/files/pdfs/publications/DP72_full.pdf>.
10. See *e.g.* Christopher Kuner et al, "Face-to-data — Another Developing Privacy Threat?" (2013) 3:1 International Data Privacy Law 1.

spaces and disappear from the foreground, projecting the human user into it".[11] The coupling of RFID technology with internet developments heralds the development of a new "Internet of Things" in which networked controls, sensors and devices for collecting data will increasingly be built into common gadgets, including household appliances, cars and the power grid, permitting "connectivity for anything".[12] The Internet of Things allows further profiling of individuals via the inanimate things with which they are associated by "subjecting more and more previously unobservable activity to electronic measurement, observation, and control".[13] Examples of this development include technologies for monitoring home wearable computing devices,[14] tools used by individuals to track their health and fitness and smart power devices.[15] Moreover, "innovation in this space is already occurring at an extremely rapid pace, thanks to the same underlying drivers of the Internet economy, namely

11. Maja Pantic et al, *Human Computing and Machine Understanding of Human Behavior: A Survey: Proceedings of the 8th International Conference on Multimodal Interfaces, Banff, 2006* (New York: ACM Publications, 2006) 239.
12. Marianna Tafich, "The Internet of Things: Application Domains" in Eckehard Steinbach et el, eds, *Advances in Media Technology: Internet of Things* (Technische Universität München, 2013) at 37 (15 January 2013), online: Advances in Media Technology <citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.395.23&rep=rep1&type=pdf>.
13. Neil M Richards, "The Dangers of Surveillance" (2013) 126:7 Harvard Law Review 1934 at 1940.
14. See Melanie Swan, "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0" (2012) 1:3 Journal of Sensor and Actuator Networks 217.
15. See Joseph Savirimuthu, "Smart Meters and the Information Panopticon: Beyond the Rhetoric of Compliance" (2013) 27:1–2 International Review of Law, Computers & Technology 161.

Moore's Law[16] and Metcalfe's Law".[17]

Developments that facilitate surveillance have a close interrelationship with decision-making practices. Surveillance technology opens up new possibilities for making use of data, while the increasingly voracious appetite for personal data is fuelling further technological innovation. As noted by Lyon, vast quantities of data are collected, stored and assessed to create profiles and risk categories with an aim toward planning, predicting and preventing "by classifying and assessing those profiles and risks".[18] This allows for more streamlined and better-targeted decision-making, but it also facilitates a level of "social sorting" that is both non-transparent and potentially discriminatory.

While these practices are by no means new, they have been taken a step further via the use of algorithms to mine the vast pools of data that are now available for analysis. As explained by Zarsky, these algorithms are used "to reveal association rules and clusters within the data that might not have been apparent to the analyst initially sifting through the information", producing results that are unpredictable for the analyst and the data subjects and facilitating the revelation of more patterns and

16. As described by Ian Brown, "Computer processing power is expected to continue following Moore's Law, doubling every 18–24 months — at least thirty-fold in the next decade, although by that point the fundamental limits of silicon engineering will be approaching": UK, Government Office for Science, *Future Identities: Changing Identities in the UK: The Next 10 Years – full report*, by Ian Brown, DR 5 (London: Foresight Future Identities, 2013), 1.2.

17. Adam Thierer, "Privacy and Security Implications of the Internet of Things" *Social Science Research Network* (1 June 2013), online: SSRN <www.ssrn.com/abstract=2273031>, at 3, n 20, citing Michael Chui, Markus Löffler & Roger Roberts, "The Internet of Things" *McKinsey Quarterly* (March 2010), online: McKinsey & Company <www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things>.

18. See David Lyon, "Surveillance as Social Sorting: Computer Codes and Mobile Bodies" in David Lyon, ed, *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (London: Routledge, 2003) at 13.

correlations.[19] These techniques are used to mine "Big Data"; that is, "datasets whose size is beyond the ability of typical database software to capture, store, manage, and analyse".[20]

III. Why Loss of Anonymity Requires Attention

Technology-facilitated surveillance is arguably a problem because it undermines the ability of individuals to remain anonymous beyond the narrow confines of private places. This, in turn, makes them potentially vulnerable to a range of harms, ranging from behavioural manipulation through to exploitation, discrimination, identity theft and stalking.

Lack of public place privacy is problematic for reasons similar to those which were identified by privacy advocates when considering the impact of the convergence of computer and telecommunications technologies.[21] These analyses focused on issues of human autonomy and dignity, the use of personal information as a basis for the exercise of power and the lack of dignity inherent in treating individuals as composites of their collated data;[22] they emphasised the important social dimension of anonymity and its role in protecting processes of self-definition and individuation.[23]

Modern observational and information collection activities undermine anonymity by making it difficult, if not impossible, to engage in any publicly observable activities free from identification and surveillance. In doing so they create "a new kind of knowledge …

---

19. Tal Z Zarsky, "*Desperately Seeking Solutions*: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society" (2004) 56:1 Maine Law Review 13 at 27.
20. James Manyika et al, *Big Data: The Next Frontier for Innovation, Competition, and Productivity* (McKinsey Global Institute, 2011) at 1.
21. See *e.g.* Moira Paterson, "Privacy Protection in Australia: The Need for an Effective Private Sector Regime" (1988) 26:2 Federal Law Review 371.
22. Austl, Commonwealth, Victorian Law Reform Commission, *Defining Privacy* (Occasional Paper) by Kate Foord (Melbourne: Victorian Law Reform Commission, 2002) at 3.
23. See Jo Ann Oravec, "The Transformation of Privacy and Anonymity: Beyond the Right to be Let Alone" (2003) 39:1 Sociological Imagination 3.

which is re-ordered, codified and made legible to rational, algorithmic understanding"[24] that in turn creates "an ability not only to define 'normal' behavior, but to spot 'abnormal' behaviour through profiling techniques".[25]

Haggerty and Ericson's concept of the "surveillant assemblage"[26] provides a useful device for understanding the nature of the surveillance practices that have arisen in response to the surveillance potential of new technologies. This complex system arises due to the converging interests of multiple public and private bodies in establishing credentials (for example, identity and other personal attributes) and surveillance systems to provide for ways to differentiate amongst unknown strangers. This system is designed to improve the efficiency of decision-making, but it is problematic to the extent that "[l]ack of public anonymity promotes conformity and an oppressive society",[27] and it encourages blandness and conformity, leading to "a blunting and blurring of rough edges and sharp lines".[28]

An alternative metaphor, suggested by Solove, is Kafka's *The Trial*, which highlights the issue of lack of control over information in a context where bureaucratic decisions are increasingly based on dehumanised information processing.[29] This metaphor is useful in emphasising that surveillance can be dangerous and oppressive, even where the intentions that underlie it are inherently benign. The danger lies in the use of surveillance as a basis for automated decision-making and the

---

24. David J Phillips, "Beyond Privacy: Confronting Locational Surveillance in Wireless Communication" (2003) 8:1 Communications Law & Policy 1 at 18.
25. *Ibid*.
26. Kevin D Haggerty & Richard V Ericson, "The Surveillance Assemblage" (2000) 51:4 British Journal of Sociology 605.
27. Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity" (2002) 72:1 Mississippi Law Journal 213 at 240.
28. Julie Cohen, "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52:5 Stanford Law Review 1373 at 1426.
29. Daniel J Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004) at 36–39.

oppressiveness that this can create in contexts where the individual is unaware of what is being collected and of the potential consequences that might follow.

The end result is what Cohen describes as a process of modulation: "a set of processes in which the quality and content of surveillant attention is continually modified according to the subject's own behavior, sometimes in response to inputs from the subject but according to logics that ultimately are outside the subject's control".[30] As she explains, the very ordinariness of this process makes it extremely powerful, producing citizens who are very different from those which form the basis for the traditional liberal democratic tradition; lack of privacy deprives them of the breathing space to engage in socially situated processes of boundary management, thereby ensuring that "the development of subjectivity and the development of communal values do not proceed in lockstep".[31] This process is not only harmful to individual autonomy but also at odds with broader public policy goals relating to liberal democratic citizenship and innovation.

IV. Existing Regulatory Frameworks and Their Shortcomings

The key regulatory frameworks that are currently used to regulate aspects of surveillance fall into four broad groups; (1) laws that regulate interception of communications; (2) laws that regulate the uses of specific surveillance devices, including listening devices; (3) data protection and other laws that require compliance with fair information handling principles; and (4) common law and statutory rights to sue in the courts.

These frameworks all suffer from a similar shortcoming to that observed by Solove in relation to the United States laws that regulate electronic surveillance: "[t]he degree of protection against certain forms

30. Julie Cohen, "What Privacy is For" (2013) 126:7 Harvard Law Review 1904 at 1915 [Cohen, "What Privacy is For"].

31. *Ibid* at 1911, citing Julie Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven: Yale University Press, 2012) at 150.

of surveillance often does not turn on how problematic or invasive it is, but on the technicalities of how the surveillance fits into the law's structure".[32]

A. Telecommunications Interception Laws

Surveillance involving the interception of telecommunications (including the accessing of communications stored within telecommunications systems) is generally regulated by telecommunications interception laws. These typically permit law enforcement and national security bodies to intercept telecommunications in specific circumstances, while making interception otherwise illegal.

In Australia, the *Telecommunications (Interception and Access) Act* prohibits: intercepting a "real-time" communication passing over the telecommunications system;[33] accessing an electronic communication such as an email, Small Message Service or voicemail message while it is stored on a telecommunications carrier's (including an Internet Service Provider's) equipment;[34] and communicating or otherwise dealing with illegally intercepted information.[35] These offences carry substantial criminal sanctions. The term "interception" is defined as listening to or recording a conversation by any means without the knowledge of the person making the communication.[36]

---

32. Daniel J Solove, "Reconstructing Electronic Surveillance Law" (2003) 72:6 The George Washington Law Review 1264 at 1298.
33. *Telecommunications (Interception and Access) Act 1979* (Cth) (Austl), ss 7(1), 105.
34. This prohibition applies in circumstances where that message cannot be accessed on that equipment by a person who is not a party to the communication, without the assistance of an employee of the carrier: *Ibid*, ss 5(1) ("stored communication"), 108.
35. *Ibid*, ss 63, 108(1).
36. *Ibid*, s 6(1) ("interception").

The equivalent federal legislation in the United States[37] makes it a federal crime for any person to intentionally intercept (or endeavour to intercept) wire, oral or electronic communications by using an electronic, mechanical or other device,[38] or to intentionally access without authorisation (or to exceed an authorisation to access) a facility through which an electronic communication service is provided and thereby obtain, alter, or prevent authorised access to a wire or electronic communication while it is in electronic storage in such a facility.[39] The term "interception" is defined as the "aural or other acquisition" of the contents of various kinds of communications by means of "electronic, mechanical or other devices",[40] and the prohibition applies both to "electronic communications", which encompass most radio and data transmissions and any communication from a tracking device,[41] and "oral communications", which include any face-to-face conversations for which the speakers have a justifiable expectation of privacy.[42]

In the case of Canada, the *Criminal Code* makes it an offence for

37. These are supplemented by state wiretap laws that are mostly directed at telephone conversations. For example, it is illegal in California to record or eavesdrop on any confidential communication, including a private conversation or telephone call, without the consent of all parties to the conversation: *California Penal Code*, PEN § 632 (2017) (US); The Citizen Media Law Project provides some selected summaries of state recording laws: The Citizen Media Law Project, "State Law: Recording" *Digital Media Law Project* (2 March 2008), online: Berkman Center for Internet & Society <www.citmedialaw.org/legal-guide/state-law-recording>; there is also a full list of state wiretap laws on the website of the National Conference for State Legislatures at: "Electronic Surveillance Laws" *National Conference of State Legislatures* (23 March 2012), online: NCSL <www.ncsl.org/programs/lis/ CIP/surveillance.htm> [*Electronic Surveillance Laws*].
38. *Electronic Communications Privacy Act*, 18 USC § 2511(1) (2006).
39. *Stored Communications Act 1986*, 18 USC § 2701(a) (2006).
40. *Ibid*, § 2510(4).
41. "Tracking Device" is defined in *ibid*, § 3117(b) as "an electronic or mechanical device which permits the tracking of the movement of a person or object'".
42. *Ibid*, § 2510(2). The meaning of "oral communications" is discussed in *United States v Larios*, 593 F Supp (3d) 82 at 92 (1st Cir 2010) (US).

anyone to "by means of any electro-magnetic, acoustic, mechanical or other device wilfully [intercept] a private communication".[43] The term "private communication" is defined broadly to include any oral communication or telecommunication, including "any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it".[44] Interception includes listening to, recording or acquiring a communication, or acquiring its substance, meaning or purport.[45]

Interception laws provide valuable protection for communications that take place over telecommunications systems, but they commonly suffer from two key defects. The first is that, in countries such as Australia and the United States, they protect only communications that involve the use of telecommunications systems, as opposed to, say, oral communications or communications via Bluetooth technology. They also typically offer differential protection based on artificial distinctions between transactional and content data, with the former receiving a much lower level of, or no, protection based on the increasingly incorrect assumption that transactional data is inherently less privacy invasive than communicative content.[46]

However, the nature and extent of metadata that can now be collected means that it can be as, or even more, revealing than content data. As noted by a former Ontario Information and Privacy Commissioner:

> Access to [metadata] will reveal the details of our personal, political, social, financial, and working lives. It provides the raw material for the creation of detailed, comprehensive, time-stamped map-lines of who is communicating with whom, when, how often, and for how long; where the senders and recipients are located; who else is connected to whom, and so forth.[47]

Research conducted at Stanford illustrates the potentially revealing nature

43. *Criminal Code*, RSC 1985, c C-46, s 184(1).
44. *Ibid*, s 183.
45. *Ibid*.
46. *Ibid*.
47. Office of the Ontario Privacy Commissioner, "A Primer on Metadata: Separating Fact from Fiction", by Ann Cavoukian, PhD, Information and Privacy Commissioner (Ontario: IPC, July 2013) at 12.

of metadata. The study involved 546 participants who ran an application on their cell phones that submitted device logs and social network information for analysis.[48] In analysing their results, the researchers commented that the degree of sensitivity relating to persons and organisations contacted by the participants had taken them aback. The persons contacted included "Alcoholics Anonymous, gun stores, NARAL Pro-Choice, labor unions, divorce lawyers, sexually transmitted disease clinics, a Canadian import pharmacy, strip clubs, and much more".[49] The researchers also discussed potential inferences that could be made from patterns of calls and referred to a number of examples, including a participant who had communicated with "multiple local neurology groups, a specialty pharmacy, a rare condition management service and a hotline for a pharmaceutical used solely to treat relapsing multiple sclerosis"[50] and another who in the space of three weeks "contacted a home improvement store, locksmiths, a hydroponics dealer, and a head shop".[51]

B. Surveillance Device Laws: Listening Devices and Beyond

Surveillance devices laws offer protection against specific uses of surveillance devices. They generally regulate uses of listening devices but may also extend more broadly to other categories of devices, including those used to track the location of individuals and items with which they are associated (such as cars) and optical surveillance devices, including CCTV cameras.

---

48. "What's in Your Metadata?" *The Center for Internet and Society* (2013), online: Stanford Law School <https://cyberlaw.stanford.edu/blog/2013/11/what%27s-in-your-metadata>.
49. Jonathan Mayer & Patrick Mutchler, "MetaPhone: The Sensitivity of Telephone Metadata" *Web Policy* (blog) (12 March 2014), online: Web Policy <www.webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/>.
50. *Ibid*.
51. *Ibid*. "Head shop" is a colloquial expression used to describe an enterprise that retails items used for the consumption of cannabis or related to the cannabis culture.

In the case of the United States, surveillance device regulation is not the norm, and listening is regulated primarily via interception laws, as discussed above, although a small number of states impose restrictions on visual surveillance.[52] For example, the *Georgia Penal Code* makes it an offence to "to observe, photograph, or record the activities of another which occur in any private place and out of public view".[53]

In contrast, surveillance device laws are commonplace at the state and territory levels in Australia.[54] For example, the Victorian *Surveillance Devices Act* contains general prohibitions against the use of listening devices, optical surveillance devices and tracking devices.[55] As in the case of telecommunications interception, these are subject to exceptions in respect of authorised activities of law enforcement and national security bodies. These are also subject to a number of restrictions that limit their operation in public places. For example, the listening device prohibition is limited by reference to a test based on reasonable expectation of being overheard,[56] the optical surveillance prohibition is limited in its application to surveillance of indoor activities and by reference to a test based on reasonable expectation of being seen[57] and the definition of

52. The website of the National Conference for State Legislatures at *Electronic Surveillance Laws*, *supra* note 37, contains details of state laws which impose restrictions on visual surveillance.
53. 11 Ga Code Ann tit 16 § 16-11-62 (2010) (US). This prohibition is subject to a number of exceptions set out in paras (A)–(C).
54. *Listening Devices Act 1992* (ACT) (Austl); *Surveillance Devices Act 2007* (NSW) (Austl); *Surveillance Devices Act* (NT) (Austl); *Invasion of Privacy Act 1971* (Qld) (Austl); *Listening and Surveillance Devices Act 2016* (SA) (Austl); *Listening Devices Act 1991* (Tas) (Austl); *Surveillance Devices Act 1999* (Vic) (Austl); and *Surveillance Devices Act 1998* (WA) (Austl).
55. *Surveillance Devices Act 1999* (Vic) (Austl), ss 6–8. Section 9 also contains a prohibition against the use of "data surveillance devices" (see definition in s 3(1)) but this is limited in its application to law enforcement officers. The prohibitions in these sections related to the installation, use and maintenance of surveillance devices and are supplemented by further prohibitions in ss 11 and 12 against the communication and publication of data wrongfully obtained via use of surveillance devices.
56. *Ibid*, ss 3(1) (definition of "private conversation"), 6(1).
57. *Ibid*, ss 3(1) (definition of "private activity"), 7(1).

tracking device is limited to devices designed solely for tracking[58] (so does not therefore apply, for example, to cell phones).

These tests are based on assumptions that are arguably no longer appropriate due to technological developments. For example, the fact that one might reasonably expect to be seen by a random passer-by does not mean that one should expect to be photographed by a distant camera equipped with face recognition technology. As observed by Boa in relation to common law tests based on reasonable expectations of privacy, "[t]echnological capabilities and the resulting information practices are constantly changing. As a result, social norms of what is reasonable have not been, and arguably cannot be, established".[59]

In the case of Canada, specific regulation of surveillance devices is likewise not the norm and listening is regulated primarily via the prohibition against interception discussed above. In addition, various uses of surveillance devices, including optical surveillance devices[60] and the use of GPS tracking devices,[61] have been held to qualify as searches, although their reasonableness will depend on the specific context.

Surveillance device laws have the advantage of being tied specifically to the devices used for surveillance but, even to the extent that they are comprehensive in terms of the types of devices covered, these laws generally offer minimal protection against surveillance in public places due to the inherent problems in finding tests that capture what matters without encroaching unduly on other competing interests. They may also be of limited assistance to the extent that they fail to encompass the full spectrum of devices that may potentially be used for the purposes of surveillance.

This issue arises most acutely in relation to optical surveillance devices due to the need to ensure that they do not impact adversely

---

58. *Ibid*, ss 3(1) (definition of "tracking device"), 8(1).
59. Kristin Boa, "Privacy Outside the Castle: Surveillance Technologies and Reasonable Expectations of Privacy in Canadian Judicial Reasoning" in David Matheson, ed, *Contours of Privacy* (Newcastle: Cambridge Scholars, 2009) 241 at 244.
60. *R v Wong*, [1990] 3 SCR 36 at para 61.
61. *R v Wise*, [1992] 1 SCR 527.

on legitimate uses of cameras. Abandonment of tests based on indoor/outdoor distinctions and reasonable expectations of being seen, raises the issue of how to distinguish between activities that are legitimate (for example, taking a photograph for personal or artistic purposes) and those that should be prohibited (for example, surreptitious filming of activities that are clearly private in nature such as long lens filming of a couple making love in a location that is secluded but outdoors).

C. Common Law and Statutory Rights of Action for Breaches of Privacy

Common law and statutory rights of action fall into two main groups. The first comprises common law rights of action based on some or all of the four United States privacy torts set out in the *Restatement (Second) of Torts*;[62] these also form the basis for most statutory rights of action in Canada.[63] The second is the extended action for breach of confidence, which has been developed by courts in the United Kingdom[64] and is

62. *Restatement (Second) of Torts* (Washington DC: American Law Institute, 1977) at §§ 657B-E [American Law Institute]; intrusion upon seclusion, appropriation of name or likeness, publicity given to private life and publicity placing person in false light.
63. For example, the Canadian provinces of British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador all have statutory privacy torts: see *Privacy Act*, RSBC 1996, c 373; *The Privacy Act*, RSS 1978, c P-24; *The Privacy Act*, RSM 1987, c P-125; *An Act Respecting the Protection of Personal Privacy*, RSNL 1990, c P-22; together referred to as ["Canadian Provincial Statutory Privacy Torts"].
64. For example, this is seen in the leading cases of *Campbell v MGN Ltd,* [2004] UKHL 22 [*Campbell*], and *Mosley v News Group Newspapers Ltd,* [2008] EWHC 1777 (QB).

currently under active consideration in Australia.[65]

In the case of the former, the intrusion tort is more obviously directed to the regulation of surveillance, as it focuses on the invasion of the private sphere (rather than on the publication of personal data)[66] and has been interpreted as being capable of extending to surveillance conducted in public places.[67] However, while it creates less obvious First Amendment issues than the public disclosure tort, it has nevertheless been construed, at least in some cases, as being subject to newsworthiness privilege.[68] The intrusion tort has been recognised recently in Canada[69] and New Zealand,[70] although it remains unclear to what extent it will be recognised as applying to public place surveillance. There are also a number of jurisdictions that have statutory intrusion torts.[71]

The other privacy tort that may be indirectly relevant is the public disclosure tort, which regulates the public disclosure of private facts, including those acquired via surveillance. However, this is generally of

65. In *Australian Broadcasting Corporation v Lenah Game Meats*, [2001] HCA 63, Gleeson CJ supported an extension of the action of breach of confidence to protect private information. While that court has yet awarded relief on this basis, the decision of the Victorian Court of Appeal in *Giller v Procopets*, [2008] VSCA 236 (Austl), has arguably further paved the way for such a development by following English case law in deciding that damages for breach of confidence can be awarded for mental distress falling short of psychiatric injury.
66. See Adam J Tutaj, "Intrusion Upon Seclusion: Bringing an 'Otherwise' Valid Cause of Action into the 21st Century" (1999) 82:3 Marquette Law Review 665.
67. See *e.g. Wolfson v Lewis*, 924 F Supp 1413 at 1433–35 (Dist Ct Pa 1996) (US). See further, Carmin L Crisci, "All the World is Not a Stage: Finding a Right to Privacy in Existing and Proposed Legislation" (2002) 6:1 New York University Journal of Legislation & Public Policy 207 at 228–30.
68. See *Dempsey v National Enquirer*, 702 F Supp 927 at 930–31 (Dist Ct Me 1988) (US). For further examples see Lyrissa B Lidsky, "Prying, Spying, and Lying: Intrusive Newsgathering and What the Law Should Do About It" (1999) 73:1 Tulane Law Review 173 at 209, n 187.
69. *Jones v Tsige,* 2012 ONCA 32.
70. *C v Holland,* [2012] NZHC 2155.
71. See *e.g.* Canadian Provincial Statutory Privacy Torts, *supra* note 63; American Law Institute, *supra* note 62.

limited assistance in relation to public place surveillance as it runs directly into conflict with freedom of expression/speech. This is a major problem in the United States due to the strength of First Amendment protection but is also an issue in New Zealand, which recognises a similar tort.[72]

It is also problematic to the extent that it contains an offensiveness test that relates to the information disseminated, as opposed to the method by which it was obtained, and ignores the dignitary harm resulting from the surveillance activities that underpin the disclosure. This issue has attracted discussion in New Zealand in the aftermath of the decision in *Andrews v Television New Zealand*[73] in which the court declined to award relief in respect of the broadcast of footage of the plaintiffs being extracted from the wreckage of their car, even though the court found that they had a reasonable expectation of privacy in relation to their conversations with each other.[74]

The extended action for breach of confidence demonstrably provides better protection for privacy in public places.[75] However, as currently formulated, it requires the disclosure of personal information and is therefore not inherently suited to the regulation of surveillance *per se*. Moreover, it does not regulate surveillance, however intrusive on privacy, if the information acquired is not disclosed to other persons.

More generally, it is arguable that privacy-based rights of action have the advantage of focussing squarely on the interest that is in issue, but they create difficulty because of the nebulous nature of privacy as a concept and the fact that it generally rubs up against other competing rights. The

---

72. See Moira Paterson, "Criminal Records, Spent Convictions and Privacy: A Trans-Tasman Comparison" (2011) 69:1 New Zealand Law Review 69 at 74–76.
73. *Andrews v Television New Zealand*, [2009] 1 NZLR 220 (HC).
74. For a useful critique on the New Zealand tort see Nicole A Moreham, "Why is Privacy Important? Privacy, Dignity and Development of New Zealand Breach of Privacy Tort" in Jeremy Finn & Stephen Todd, eds, *Law, Liberty, Legislation: Essays in Honour of John Burrows, QC* (Wellington: LexisNexis, 2008), online: Victoria University of Wellington <www.victoria.ac.nz/law/pdf/nm-law-liberty-legislation.pdf>.
75. This is evident from the outcomes in *Campbell, supra* note 64, and *Murray v Big Pictures (UK) Ltd*, [2008] EWCA Civ 446.

problem, therefore, lies in devising a test that is sufficiently certain and at the same time strikes an appropriate balance between privacy and other competing rights, such as freedom of expression/speech.

D. Data Protection Laws and Other Laws Based on Fair Information Practices ("FIPs")

Data protection laws protect privacy by requiring compliance with FIP-based rules that regulate the handling of personal information. They are relevant to surveillance insofar as they impose limitations on the collection (and subsequent use of) personal information. Instead of being based on the type of device or communication system being used to collect data, they focus on the nature of the data in question and whether or not it relates to an individual who is identified or potentially identifiable. Schwartz & Solove refer to this concept as "personally identifiable information".[76]

The concept of regulation via fair information principles has its origins in the United States in a report by the Advisory Committee on Automated Personal Data Systems in the Department of Health, Education and Welfare.[77] These principles formed the basis for the public sector regime in the *Privacy Act* in the United States[78] and also for the

76. Paul M Schwartz & Daniel J Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Data" (2011) 86:6 New York University Law Review 1814.
77. US, Department of Health, Education and Welfare, *Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computes and the Rights of Citizens* (No (OS) 73-94) (Washington DC: DHEW Publication, 1973).
78. 5 USC § 552a (1974) [US *Privacy Act*].

Safe Harbor principles[79] administered by the Federal Trade Commission, as well as for the many data protection regimes that exist throughout the world.[80]

The United States is unusual in terms of its lack of any FIP-based regime of general application to the private sector, although the FIPs form the basis for many federal and state laws[81] and are summarised in set of principles developed by the FTC to provide guidance concerning privacy-friendly, consumer-oriented data collection practices.[82]

The federal public sector *Privacy Act*[83] regulates information handling by federal agencies via a Code of Fair Information Practice.[84] It requires inter alia that agencies must "collect information to the greatest extent practicable directly from the subject individual when the information

---

79. Full details about this regime can be accessed online: US, Federal Trade Commission, "U.S.-E.U Safe Harbor Framework" (FTC, 25 July 2016), online: FTC <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework>. It should be noted that the Safe Harbor Framework is no longer legally recognised as adequate under EU law for transferring personal data to the US and that the US and EU have now negotiated a new Privacy Shield Network, see "Privacy Shield Framework" *International Trade Administration*, online: ITA <https://www.privacyshield.gov/welcome>. The latter contains further additional protections.
80. For a useful overview of the evolution of laws based on FIPs see Fred Cate, "The Failure of Fair Information Practice Principles" in Jane K Winn, ed, *Consumer Protection in the Age of the 'Information Economy'* (Abingdon: Taylor and Francis, 2006) 341 [Cate, "Fair Information Practice Principles"].
81. See *e.g. The Fair Credit Reporting Act,* 15 USC § 1681 (1970); *Right to Financial Privacy Act,* 12 USC § 3401 (1978); *Electronic Communications Privacy Act* of 18 USC §§ 2510-252 (1986). For a useful overview of a number of FIP-based laws in the US, see Schwartz & Solove, *supra* note 76.
82. US, Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998) at 7–14.
83. US *Privacy Act*, *supra* note 78.
84. US, Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Data Systems, Records, Computers, and the Rights of Citizens, *Code of Fair Information Practice* (HEW, July 1973).

may result in adverse determinations about an individual's rights, benefits, and privileges under any Federal program".[85] It also prohibits the maintenance of any record "describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity".[86]

The *Privacy Act* generally applies only to systems of records — i.e. "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual".[87] The term "record" is defined as:

> [A]ny item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.[88]

In *Albright v United States*[89] the court held that a videotape of a meeting qualified as record as it contained a means of identifying an individual by picture or voice and that it contravened the *Act* by showing an individual exercising their First Amendment rights (by making complaints about their employment).[90] The court also held that it did not matter in that case that the videotape was not maintained in a system of records, as this specific prohibition applied to agencies more generally.

In Australia, the *Privacy Act*[91] was once similarly confined to the

85. US *Privacy Act*, *supra* note 78**,** § 552a(e)(2).
86. *Ibid***,** § 552a(e)(7).
87. *Ibid***,** § 552a(a)(5).
88. *Ibid*, § 552a(a)(4).
89. 631 F (2d) 915 at 920 (DC Cir 1980) (US).
90. This case is discussed in Robert Gellman, "A General Survey of Video Surveillance Law in the United States" in Sjaak Nout, Berend de Vries & Corien Prins, eds, *Reasonable Expectation of Privacy?: Eleven Country Reports on Camera Surveillance and Workplace Privacy* (The Hague: TMC Asser Press, 2005) 7.
91. *Privacy Act 1988* (Cth) (Austl) [Austl *Privacy Act*].

public sector, but it now applies also to the private sector and has recently been amended to include a single set of *Australian Privacy Principles* ("*APPs*") that apply to information handling by both sectors.[92] The application of the *APPs* to the private sector is, however, subject to a large number of exceptions, including exceptions for the journalistic practices of media organisations[93] and for acts of individuals acting in a non-business capacity.[94]

The *APPs* govern the handling of "personal information", which is defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable.[95] This is a new definition[96] that has been designed to require "a consideration of the cost, difficulty, practicality and likelihood that the information will be linked in such a way as to identify [the individual]".[97] This has the effect that the records of surveillance are not covered by the *Act* unless they contain images or other data that allow for recognition of the individuals to which

92. The *Privacy Act* is supplemented by laws that operate in a similar way in relation to most government agencies in most states and the Northern Territory: *Privacy and Personal Information Protection Act 1998* (NSW) (Austl); *Information Act 2000* (NT) (Austl); *Information Privacy Act 2009* (Qld) (Austl); *Personal Information Protection Act 2004* (Tas) (Austl); *Privacy and Data Protection Act 2014* (Vic) (Austl). There is a detailed overview of the Privacy Act in Moira Paterson, "Privacy" in Matthew Groves, ed, *Modern Administrative Law in Australia: Concepts and Context* (Port Melbourne: Cambridge University Press, 2014).
93. Austl *Privacy Act*, *supra* note 91, s 7B(4).
94. *Ibid*, s 7B(1).
95. *Ibid*, s 6(1).
96. It was amended by the *Privacy Amendment (Enhancing Privacy Reform) Act 2012* (Cth) (Austl).
97. Austl, Commonwealth, Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108) (ALRC, 2008) at 6.57. This approach is consistent with that taken by the Victorian Civil and Administrative Tribunal in interpreting a similar (but not identical) provision in the *Information Privacy Act 2000* (Vic) (Austl): See *WL v La Trobe University*, [2005] VCAT 2592 (Austl). For a further discussion of the Australian provisions, see Mark Burdon & Paul Telford, "The Conceptual Basis of Personal Information in Australian Privacy Law" (2010) 17:1 Murdoch University, Electronic Journal of Law 1.

they relate, or unless they have been collected in a context in which the collecting organisation can readily link them to other data that identifies an individual.

This issue has arisen for consideration in recent litigation concerning an application made under the *Privacy Act* for access to the applicant's mobile network data. In *Telstra Corporation Ltd v Privacy Commissioner*, the Commonwealth Administrative Appeals Tribunal found against the applicant on the ground that this data did not constitute "personal information".[98] In the tribunal's view, the metadata in question was "all about the way in which Telstra delivers the call or the message. That is not about Mr Grubb".[99] This decision was upheld by the Full Court of the Federal Court of Australia, which expressed the view that the words "about an individual" in the definition of personal information raised a threshold question that needed to be addressed before it could be determined whether that individual is identified or identifiable.[100] In the court's view, it was necessary in every case to consider whether each item of personal information requested, individually or in combination with other items, was "about an individual". This would "require an evaluative conclusion, depending upon the facts of any individual case, just as a determination of whether the identity [could] reasonably be ascertained will require an evaluative conclusion".[101]

The *APPs* include a collection limitation principle, which requires that personal information be collected fairly and legally[102] and precludes the collection of personal information unless it is reasonably necessary for one or more of the functions or activities of the organisation collecting it.[103] They also include further principles relating to open and transparent

98. [2015] AATA 991.
99. *Ibid* at para 112.
100. *Privacy Commissioner v Telstra Corporation Ltd*, [2017] FCA 4 at para 89.
101. *Ibid* at para 63; See also Normann Witzleb, "'Person Information' under the Privacy Act 1988 (Cth) – Privacy Commissioner v Telstra Corporation Ltd [2017] FCAFC 4" (2017) 45:2 Australian Business Law Review 188.
102. *Australian Privacy Principles, APP* 3.5, being Schedule 1 of the *Privacy Act 1988* (Cth) (Austl).
103. *Ibid*, *APP* 3.2.

management,[104] notification of the collection of personal information,[105] limitations on use and disclosure,[106] requirements to maintain security[107] and integrity[108] and obligations to provide access to information subjects.[109]

Oversight of the *Privacy Act* is provided by the Office of the Australian Information Commission. The Commissioner's functions are grouped within the Act according to whether they foster compliance (via the provision of guidance),[110] monitor compliance[111] or support compliance (via the provision of advice).[112] The Act is enforced primarily via a complaints-based system, although the Information Commissioner also has power to conduct audits to assess entities' maintenance of personal information,[113] to require provision of privacy impact assessments[114] and to conduct "own motion" investigations.[115]

Canada differs in that it has separate federal privacy regimes. The *Privacy Act*[116] and the *Personal Information Protection and Electronic Documents Act*[117] govern the information handling practices of the federal government and private organisations, respectively. These both require compliance with sets of FIPs that apply in respect of "personal information". The latter is defined as "information about an identifiable

104. *Ibid, APP* 1.
105. *Ibid*, *APP* 5.
106. *Ibid*, *APP* 6.
107. *Ibid*, *APP* 10.
108. *Ibid*, *APP* 11.
109. *Ibid*, *APP* 12.
110. *Ibid*, s 28.
111. *Ibid*, s 28A.
112. *Ibid*, s 28B.
113. *Ibid*, s 33C.
114. *Ibid*, s 33D(1); A "privacy impact assessment" means a written assessment that identifies the impact an activity or function might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating that impact: Also see *ibid*, s 33D(3).
115. *Ibid*, s 40.
116. *Privacy Act*, RSC 1985, c P-21 [Canada *Privacy Act*].
117. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].

individual".[118] Both Acts are subject to oversight by the Office of the Privacy Commissioner of Canada.

A problem with laws based on FIPs is that they depend on the criterion of personally identifiable information ("PII") to establish their boundaries. As explained by Schwartz and Solove, without these boundaries "privacy rights would expand to protect a nearly infinite array of information, including practically every piece of statistical or demographic data".[119] However, the criterion of identifiability is inherently fluid and whether or not information is reasonably identifiable depends on how much effort is put into the process, to what extent linkage with other available information is relevant and the extent to which it is appropriate to consider new and emerging identification technologies. Furthermore, determining where precisely to set the boundaries for identifiability raises difficult policy issues given that information that qualifies as personal information is generally subject to the full spectrum of requirements set out in the legislation.

Take, for example, a CCTV image of someone who is not immediately identifiable but who may be identified if face recognition technology is applied to the footage. From a privacy perspective, collection *per se* is of minimal privacy invasiveness if the footage is simply kept for a period to determine if it is required, say, to assist in the detection of pilfering, and then disposed of without that individual ever having been identified. However, if that image qualifies as personal information based on the fact that the individual could be identified, the collector would be required to provide access to it on request — a requirement which might be quite onerous depending on the ease of location of the image required and the need to protect the identities of any other persons who feature in the same footage (assuming that their images also qualify as personal information). On the other hand, if it does not qualify as personal information, the collector will not be under any obligation to keep the footage secure and would not be precluded from disclosing it to another individual who may have some means of recognising the individual.

---

118. Canada *Privacy Act*, *supra* note 116, s 3; *PIPEDA*, *ibid*, s 2(1).
119. Schwartz & Solove, *supra* note 76 at 1866.

A test based on identifiability also creates problems for the reasons suggested by Ohm — *i.e.* that the science of reidentifiability increasingly undermines processes of anonymization by deleting from information personal identifiers such as names and context specific identifiers such as identity numbers, account numbers, etc.[120] Millard and Hon have likewise commented that "scientific and technological advances are making it increasingly simple to de-anonymise data to 're-identify' individuals, notwithstanding the use of methods such as aggregation or barnardisation"[121] and that this may mean that "almost all data could qualify as 'personal data', thereby rendering PII meaningless as a trigger for data protection obligations".[122]

Another issue identified by Cate is that the effectiveness of current FIP-based laws depends on a control-based system that relies on procedures designed to maximise individual control, for example, via requirements for notice and consent.[123] However, consent has become an increasingly artificial construct given the complexity of the "surveillant assemblage" and the fact that individuals have little prospect of understanding the significance of individual data disclosures. Furthermore, "[n]otices are frequently meaningless because individuals do not see them or choose to ignore them, they are written in either vague or overly technical language, or they present no meaningful opportunity for individual choice".[124]

---

120. Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57:6 UCLA Law Review 1701.
121. Barnardisation is "[a] method of disclosure control for tables of counts that involves randomly adding or subtracting 1 from some cells in the table": See online: "Glossary of Statistical Terms" *Organisation for Economic Co-operation and Development* (9 November 2005), online: OECD <stats.oecd.org/glossary/detail. asp?ID=6887>.
122. Christopher Millard & W Kuan Hon, "Defining 'Personal Data' in E-Social Science" (2011) 15:1 Information, Communication & Society 66 at 77.
123. Cate, "Fair Information Practice Principles", *supra* note 80 at 341.
124. *Ibid* at 3.

V. The Significance of Constitutional/Human Rights Frameworks

A difficulty in providing effective regulation of public place surveillance is that laws that provide strong privacy protections may be viewed as undermining the freedom of the press/freedom of speech to the extent that they restrict the surveillance that facilitates the dissemination of personal information about individuals.

Constitutional frameworks play an important role in determining the nature and extent of the privacy regulation that is possible. This is most evident in the United States, where the strength of the First Amendment protection of free speech and the lack of equivalent protection of informational privacy beyond the specific context of search and seizure creates major difficulties. It is also the case in other countries, such as Canada[125] and New Zealand,[126] which have human rights laws that lack express privacy guarantees. The European Human Rights regime, which provides specific protection for privacy, as well as for freedom of expression, provides greater flexibility.[127]

However, it is arguable that the interests served by effective regulation of surveillance are in many cases identical to those which underlie the important right to free speech. As identified many years ago by Regan, privacy has suffered due to its conception as an individual right, which

125. The *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act, 1982,* being Schedule B to the *Canada Act 1982* (UK), 1892, c 11, contains a right to "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication" (s 2(b)) and a right "to be secure against unreasonable search or seizure (s 8), but no general right to privacy".

126. The *New Zealand Bill of Rights Act 1990* (NZ), 1990/109 contains a right to "freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind in any form" (s 14) and a right to be "secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise" (s 21), but not any right to privacy more generally.

127. *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 UNTS 221 at 223 arts 8–10 (entered into force 3 September 1953).

means that it fares badly when it conflicts with competing rights that are traditionally conceived of as serving broader public purposes.[128]

The individualistic view of privacy is frequently articulated in the language of a negative freedom (*i.e.* as a freedom from interference by other people)[129] and one that is in essence "anti-social" and pertaining to the "right of an individual to live a life of seclusion and anonymity, free from the prying curiosity which accompanies both fame and notoriety".[130] However, privacy may equally be conceived of as a positive claim to a status of personal dignity, premised on the ability to exercise some element of control over one's own personal information. In that sense it is not "simply an absence of information about us in the minds of others. Rather, it is the control we have over information about ourselves".[131]

Moreover, while there can be no doubt that a right to privacy is an integral feature of liberal democratic systems that value individual autonomy and dignity (in particular, the right to be treated as a human being and not some abstract object), privacy also serves broader societal goals. As explained by Raab, in the context of surveillance, lack of privacy disrupts communication, resulting in an isolation that is inconsistent with democracy;[132] "participatory freedoms require a degree of privacy" (as illustrated by the nexus between free elections and secret ballots).[133]

It follows, therefore, that it is erroneous to conceive of anti-surveillance laws as necessarily contravening free speech protection or overstepping a permissible balance between privacy and freedom of expression. That is

---

128. Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (North Carolina: University of North Carolina Press, 1995).
129. See Isaiah Berlin, "Two Concepts of Liberty" in Isaiah Berlin, ed, *Four Essays on Liberty* (Oxford: Oxford University Press, 1969) 15, online: University of Hamburg <www.wiso.unihamburg.de/fileadmin/wiso_vwl/johannes/Ankuendigungen/Berlin_twoconceptsofliberty.pdf>.
130. Louis Nizer, "The Right of Privacy: A Half Century's Developments" (1941) 39:4 Michigan Law Review 526 at 528.
131. Charles Fried, "Privacy" (1968) 77:3 Yale Law Journal 475 at 482.
132. Charles Raab, "Privacy, Democracy, Information" in Brian Loader, ed, *The Governance of Cyberspace: Politics, Technology and Global Restructuring* (London: Routledge, 1997) 153 at 157.
133. *Ibid* at 160.

not to suggest that there is not potential conflict between the two, rather that it is important to bear in mind that failure to prevent the process of modulation described by Cohen in many respects renders meaningless the protection of the right to speech.

VI. Insights From Regulatory Theory

The theory of responsive regulation developed by Ayers and Braithwaite contends that:

> the achievement of regulatory objectives is more likely when agencies display both a hierarchy of sanctions and a hierarchy of regulatory strategies of varying degrees of interventionism. ... Regulators will do best by indicating a willingness to escalate intervention up those pyramids or to deregulate down the pyramids in response to the industry's performance in securing regulatory objectives.[134]

This is further explained on the basis that "[t]he pyramidal presumption of persuasion gives the cheaper, more respectful option a chance to work first. More costly punitive attempts at control are thus held in reserve for the minority of cases where persuasion fails".[135] The regulatory pyramid[136] therefore has softer measures such as warnings, persuasion and collaboration at its base, followed by civil sanctions and then criminal sanctions at its apex.

Telecommunications interception and surveillance device laws generally rely on the impositions of criminal sanctions. These have a strong deterrent effect but require a high standard of proof for convictions and rely on police for their enforcement**.** This is not necessarily conducive to good outcomes, as illustrated by the Murdoch media scandal in the United Kingdom. The regulatory pyramid suggests that criminal sanctions should be used only as a last resort in respect of more egregious conduct and that they are inherently unsuitable as a sole or primary device for achieving across-the-board regulatory outcomes in

134. Ian Ayers & John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford: Oxford University Press, 1992) at 5–6.
135. John Braithwaite, "Responsive Regulation and Developing Economies" (2006) 34:5 World Development 884 at 887.
136. Ayers & Braithwaite, *supra* note 134 at 39.

the surveillance context.

Common law and statutory torts focus instead on providing appropriate remedies for individuals who are adversely affected by non-compliance. However, they produce a deterrent effect only to the extent that individuals are able to identify those responsible for privacy breaches that have caused (or are likely to cause) them harm and are then willing to litigate, bearing in mind that litigation may of itself be harmful to their privacy. Also they are likely to have a deterrent effect only if the damages available are sufficiently large to outweigh the potential profits to be gained from non-compliance. Furthermore, the fact these torts are available only to provide redress in respect of the types of harm that are capable of attracting legal compensation means that they are not well suited to addressing the harms inherent in the processes of modulation. It is arguable, therefore, that this purely private focus limits their usefulness as a sole or primary device for regulating surveillance.

On the other hand, data protection regimes provide for a more flexible range of regulatory options, including ones at the softer end of the spectrum (for example, education and persuasion) and scope for remedial action that is not based on individual action. Depending on how they are structured, they may include regulators with broad powers, including powers to conduct own motion investigations and to provide compensation, as well as civil and criminal penalties for more egregious or harmful conduct. They therefore offer broad scope for a regulatory solution that incorporates a pyramid of enforcement measures; one which can be tailored to address both the private and the broader public harms created by untrammelled public place surveillance.

VII. A Suggested Way Forward

The flexibility inherent in data protection regimes suggests that they offer the best starting point for regulation of surveillance, provided that they include independent regulators who have a range of softer and harder enforcement powers at their disposal and who are both able, and prepared to make use of, their more coercive powers in those instances where the softer measures have failed to elicit compliance. As noted by Ayers and Braithwaite:

> [T]he greater the heights of tough enforcement to which the agency can escalate (at the apex of its enforcement pyramid), the more effective the agency will be at securing compliance and the less likely that it will have to resort to tough enforcement. Regulatory agencies will be able to speak more softly when they are perceived as carrying big sticks.[137]

It is also important to find means of addressing the weaknesses identified above, and especially the issue of PII. As noted above, whether or not information qualifies as PII provides the touchstone for the application of an entire set of FIPs, including limitations on collection, use and disclosure, security requirements and obligations to provide rights of access and amendment. Their wording and interpretation therefore remain a matter of continuing controversy.

A prime example is the decision of the United Kingdom Court of Appeal in *Durant v Financial Services Authority*,[138] in which the expression "personal data" in the *Data Protection Act*[139] was interpreted as requiring an assessment of relevance or proximity to an individual. This, in turn, required assessment of whether the information is "biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations";[140] and whether it has "the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest".[141]

This test has been legitimately criticised on the basis that it eliminates the key obligations imposed under the *Data Protection Act*, including "fair processing, data security and no unreasonable data retention" as well as the rights of persons whose images are collected to control how they

137. *Ibid* at 6.
138. [2003] EWCA Civ 1746 [*Durant*].
139. *Data Protection Act 1988* (UK), c 29.
140. *Durant*, *supra* note 138 at para 28.
141. *Ibid*. See further Lilian Edwards, "Taking the 'Personal' Out of Personal Data: *Durant v FSA* and its Impact on the Legal Regulation of CCTV" (2004) 1:2 Script-ed 346.

are processed.[142] However, it is arguable that the test made sense in the context of the specific situation in which the applicant was requesting access to all documents in which he was featured and that the preferable way forward is to incorporate different tests based on the specific practices that are in issue and their potential privacy implications for information subjects.

Schwartz and Solove take a similar approach in arguing for reconceptualization of PII tests to resolve the reidentification issues identified by Ohm. They propose the development of a new model termed "PII 2.0", which provides different regulatory regimes for information about identified and identifiable individuals.[143] They suggest that, while all of the FIPs should apply to information about identified individuals, only some should apply to identifiable data.[144] They further suggest that "[f]ull notice, access, and correction rights should not be granted to an affected individual simply because identifiable data about her are processed" and also that "limits on information use, data minimalization, and restrictions on information disclosure should not be applied across the board to identifiable information".[145]

This suggests a useful way forward, although the distinction between identified and identifiable is a blunt one and fails to answer the question: identified by whom and in what circumstances? What is important at the end of the day is whether or not data collected is handled in ways that pose an actual or potential threat to the data subject.

Take, for example, the hypothetical scenario of a marine researcher who incidentally captures images of Angelina Jolie on a boat when collecting images of wave movements from a fixed camera. It is arguable that the researcher should not be subject to collection limitation, access and amendment principles, although they should be required either to redact the images or to hold them securely. On the other hand, the researcher

142. Lilian Edwards, "Switching Off the Surveillance Society? Legal Regulation of CCTV in the United Kingdom" in Nout, de Vries & Prins, *supra* note 90 at 101.
143. Schwartz & Solove, *supra* note 76.
144. *Ibid*.
145. *Ibid* at 1880.

should be subject to a broader range of principles if he or she wishes to use the images or disclose them to others. The key objective of this approach is to ensure that data that can potentially identify an individual receives protection only where necessary to protect the individual's privacy and also to provide an incentive to organisations to deidentify or destroy such data where it is not collected for the purpose of collecting information about the individual. It is important to remember that the appropriate disposal of personal data once it is no longer required for the purposes for which it was collected is fundamental for the protection of privacy, although it strikes at the underlying rationale of the Big Data movement.

Departure from the current "one size fits all" approach may also provide a useful way forward in dealing with the problem that the use of privacy invasive technology is no longer the sole domain of governments and business organisations. FIP-based regimes are currently ill-suited to the regulation of the non-business activities of individuals. However, there may be scope for the development of a more simplified set of principles that focus on privacy invasive uses and disclosures of personal information.

A second major issue identified by Cate is that most FIP-based regimes rely heavily on notice and content requirements, resulting in "an avalanche of notice and consent requirements" that are generally ignored.[146] He has therefore proposed an alternative set of rules based on principles of harm prevention, benefit maximisation and consistent protection.[147] Building on this approach, Cate, Cullen and Schonberg have proposed a revised set of OECD Guidelines, which have been informed by a working group organised by the Oxford Internet Institute on behalf of Microsoft.[148]

Cate's approach is to try and shift the emphasis away from control by data subjects and onto accountability on the part of the organisation

146. Cate, "Fair Information Practice Principles", *supra* note 80 at 361.
147. *Ibid* at 370–74.
148. Fred H Cate, Peter Cullen & Victor Mayer-Schönberger, "Data Protection Principles for the 21st Century: Revising the 1980 *OECD* Guidelines" *Oxford Internet Institute* (March 2014), online: OII <www.oii.ox.ac.uk/news/?id=1013>.

involved in handling personal data. It also, however, reduces existing limitations on the secondary uses of data and imposes regulation only to the extent that information handling is clearly harmful to information subjects. In that sense, it shifts the balance in favour of Big Data while retaining a safety net to catch activities that are clearly harmful and disproportionate in their privacy invasiveness.

This development has been criticised by Cavoukian, Dix and El Eman[149] on the basis that diluting consent requirements weakens privacy protection. They acknowledge the modern reality that individuals are not only confused by lengthy privacy notices but often also unaware of the data collection taking place or that they may be completely absent from the transaction which requires the processing of their data. However, they point out that depriving individuals of control over the purposes for which their personal data is collected and used is not beneficial to them; "it makes them vulnerable to the judgement exercised by others — corporate and bureaucratic systems that already affect our lives, and over which we have little or no control".[150] They also highlight that "greater reliance on law and regulation alone to police "after-the-fact" abuses of personal data is a misguided strategy; and … that there is little consensus on defining "harms" or ways in which to measure or mitigate privacy harms".[151]

Cavoukian and her co-authors suggest instead "a more robust user-centric "Transparency and Control" model"[152] based on seven principles of "Privacy by Design". Their concept of "Privacy by Design" is based on the view that "[p]rivacy and data protection should be incorporated into networked data systems and technologies by default, and become integral to organizational priorities, project objectives, design processes, and

149. Canada, Information and Privacy Commissioner, *The Unintended Consequences of Privacy Paternalism*, by Ann Cavoukian, Alexander Dix & Khaled El Emam (Toronto: 5 March 2014), online: University of Toronto <www.comm.utoronto.edu/~dimitris/JIE1001/levin4.pdf>.

150. *Ibid* at 4.

151. *Ibid* at 2.

152. *Ibid* at 13.

planning operations".[153] "Privacy by Design" has the advantage that it imposes responsibility on those involved in the collection and processing of data to build in measures to protect the privacy of individuals and is embodied as a requirement in the *General Data Protection Regulation*, which will commence operation in the European Union in May of 2018.[154] However, there is still a lack of clarity as what precisely this concept requires, and there are difficulties in implementing it in a context where it is inherently difficult to reconcile privacy interests with the interests of the Big Data movement.

A different approach based on the so-called "Right to be Forgotten" involves conferring on individuals specific rights to require the erasure of their personal information.[155] This has some potential to restore some measure of control to the individual and is embodied as a requirement in the *General Data Protection Regulation*.[156] However, a key shortcoming is that it relies on the individual for enforcement. This is problematic in a context where individuals are unaware of what information has been collected about them and how it is being used.

It is suggested that a different approach which may hold promise, is to improve the transparency not just of the different aspects of information handling but also of the outcomes of that process. The process of modulation described by Cohen[157] is harmful, at least in part, because

---

153. *Ibid* at 15.
154. EC, *Data Protection Regulation (EC) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1 [*General Data Protection Regulation*]. It is required under art 25 in respect of "potentially high-risk processing activities".
155. For a useful discussion of the advantages of such a right, see Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press, 2009).
156. *General Data Protection Regulation*, *supra* note 154. Article 17 confers a right of erasure in specific circumstances, including where the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.
157. Cohen, "What Privacy is For", *supra* note 30.

of its normalisation and the fact that individuals are unaware of the extent to which they are being manipulated. The provision of additional information at that stage (for example, informing individuals who are the subject of targeted advertising of why it is that they are receiving specific advertisements) might go some way towards alleviating these issues.

Providing increased transparency creates practical difficulties that are magnified in the context of activities based on Big Data Analytics, due to the complexities associated with making transparent the algorithms that are used to inform those activities. However, the fact that this task is difficult does not mean that it should not be attempted given the seriousness of the potential harm involved. Improving the transparency of the end products of surveillance arguably has the potential to produce more informed decision-making on the part of individuals than notices given at the point of information collection.