SURVEILLANCE, BIG DATA AND DEMOCRACY: LESSONS FOR AUSTRALIA FROM THE US AND UK

MELISSA DE ZWART,* SAL HUMPHREYS** AND BEATRIX VAN DISSEL***

In the era of big data, where people find themselves surveilled in ever more finely granulated aspects of their lives, and where the data profiles built from an accumulation of data gathered about themselves and others are used to predict as well as shape their behaviours, the question of privacy protection arises constantly. In this article we interrogate whether the discourse of privacy is sufficient to address this new paradigm of information flow and control. What we confront in this area is a set of practices concerning the collection, aggregation, sharing, interrogation and uses of data on a scale that crosses private and public boundaries, jurisdictional boundaries, and importantly, the boundaries between reality and simulation. The consequences of these practices are emerging as sometimes useful and sometimes damaging to governments, citizens and commercial organisations. Understanding how to regulate this sphere of activity to address the harms, to create an infrastructure of accountability, and to bring more transparency to the practices mentioned, is a challenge of some complexity. Using privacy frameworks may not provide the solutions or protections that ultimately are being sought.

This article is concerned with data gathering and surveillance practices, by business and government, and the implications for individual privacy in the face of widespread collection and use of big data. We will firstly outline the practices around data and the issues that arise from such practices. We then consider how courts in the United Kingdom ('UK') and the United States ('US') are attempting to frame these issues using current legal frameworks, and finish by considering the Australian context. Notably the discourse around privacy protection differs significantly across these jurisdictions, encompassing elements of constitutional rights and freedoms, specific legislative schemes, data protection, anti-terrorist and criminal laws, tort and equity. This lack of a common understanding of what is or what should be encompassed within privacy makes it a very fragile creature indeed.

* Associate Professor, Adelaide Law School, University of Adelaide.
** Senior Lecturer, Discipline of Media, University of Adelaide.
*** Research Assistant, Adelaide Law School, University of Adelaide.

On the basis of the exploration of these issues, we conclude that current laws are ill-equipped to deal with the multifaceted threats to individual privacy by governments, corporations and our own need to participate in the information society.

I PRACTICES

In this Part, we consider how information about people is now subjected to new practices brought about through the networked digital communications that have become prevalent in the lives of most people.

'[T]he power of personal information lies at the heart of surveillance.'[1] Surveillance can be described as 'the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction.'[2] In Deleuzian terms, in the surveillance society, surveillance (and therefore control) is a cumulative process of interlocking networks and 'relies on historical data to forge new visibilities.'[3] A key aspect of this new 'age of surveillance' is lack of clear differentiation between surveillance by (or on behalf of) governments and that conducted by commercial entities. 'Public- and private-sector surveillance are intertwined – they use the same technologies and techniques, they operate through a variety of public/private partnerships, and their digital fruits can easily cross the public/private divide.'[4] Due to the proliferation of services, and the complexity of regulatory regimes, agencies increasingly seek to automate their decisions.[5] Automated systems are thought to ensure consistent decisions as the rules are interpreted in the same way in every case.[6] Whether the algorithmic rules and the available data upon which the rules are based are accurate is often obscured behind a discourse of technological objectivity.

The inferential techniques used to analyse the information can provide accurate and timely insights into complicated issues.[7] However, as Citron observes, the 'opacity of automated systems shields them from scrutiny' as

1 Neil M Richards, 'The Dangers of Surveillance' (2013) 126 *Harvard Law Review* 1934, 1953.
2 David Lyon, *Surveillance Studies: An Overview* (Polity Press, 2007) 14.
3 Karl Palmås, 'Predicting What You'll Do Tomorrow: Panspectric Surveillance and the Contemporary Corporation' (2011) 8 *Surveillance & Society* 338, 342, citing Gilles Deleuze, 'Postscript on the Societies of Control' (1992) 59 *October* 3, 5–6.
4 Richards, above n 1, 1958.
5 Danielle Keats Citron, 'Technological Due Process' (2008) 85 *Washington University Law Review* 1249, 1258; James Grimmelmann, 'Regulation by Software' (2005) 114 *Yale Law Review* 1719, 1734.
6 See Citron, above n 5, 1253 citing William D Eggers, *Government 2.0: Using Technology to Improve Education, Cut Red Tape, Reduce Gridlock, and Enhance Democracy* (Rowman & Littlefield Publishers, 2005) 113.
7 David Bollier, 'The Promise and Peril of Big Data' (Aspen Institute, 2010) 2.

'citizens cannot see or debate these new rules',[8] and algorithmic decision-making based on data raises issues of 'technological due process'.[9]

A Collection

Data collection has become almost ubiquitous – it is carried out in public spaces and in private spaces. People sometimes volunteer their information and sometimes it is harvested from their actions without them knowing. Thus a person may fill out a form online and give information about themselves to a commercial or government organisation – usually in exchange for some kind of goods or services. However, volunteering this information is not necessarily a sign that they have consented to the ways in which it is used.[10] As Solove points out, the downstream uses of data may not be known to the person, particularly as their data may be aggregated with other data over time.[11] The privacy policies of many collecting sites often include terms that indicate they share information with third parties and cannot control what those third parties do with the information.[12] Control of its uses is basically lost at the point of sharing. Interestingly, the people who hold and deploy the data may not know its uses if it is subjected to algorithms that interrogate it using automated and computationally generated processes – a practice discussed further below.

Data can also be collected involuntarily or covertly in many places and through many practices. Public places are not only under surveillance through technologies such as closed-circuit television ('CCTV') cameras, but also increasingly through scanning technologies which, for instance, may collect data from peoples' mobile phones as they pass through a space.[13] Phones may be open through Bluetooth and wi-fi networks. A phone that is automatically scanning for a wireless network as a person walks through a mall can be read for information about many other activities – global positioning system ('GPS') location data may be read for information about where that person has been, contact lists may be harvested and so on. Radio frequency identification ('RFID') tags may be

8 Citron, above n 5, 1254.

9 Ibid 1258.

10 Alice E Marwick, 'How Your Data Are Being Deeply Mined' (2014) 61(1) *New York Review of Books* <http://www.nybooks.com/articles/archives/2014/jan/09/how-your-data-are-being-deeply-mined/>.

11 Daniel Solove, 'Introduction: Privacy, Self-Management and the Consent Dilemma' (2013) 26 *Harvard Law Review* 1880, 1889–90.

12 For instance, the privacy policy on the website for popular games company Blizzard contains the following statement: 'Please be aware that we cannot control the activities of third parties to whom we provide data, and as such we cannot guarantee that they adhere to the same privacy and security procedures as Blizzard.': Blizzard Entertainment, *Privacy Policy* (2014) <http://us.blizzard.com/en-us/company/about/privacy.html>.

13 Mark Burdon, 'Mobile Phone Tracking: It's Not Personal', *The Conversation* (online), 11 March 2014 <http://theconversation.com/mobile-phone-tracking-its-not-personal-23015>.

embedded in clothing purchases, giving off readable information about purchasing choices and tastes.[14]

What have traditionally been thought of as private places and interactions have also become the source of much data gathering. Governments and commercial organisations collect data from phone calls, online interactions of both a social and a commercial nature and so on. Most people are not voluntarily giving up this data, but it is almost impossible to prevent its collection.[15]

B Aggregation

The collection of individual data with respect to one phone call or one website visit may not appear to be a particularly sinister experience (and in fact we are used to being regularly warned about 'cookies' collecting information when we access a website).[16] However, even information regarding one transaction may reveal a lot about the customer (for example, calling hotlines dealing with domestic violence, suicide, depression or drug addiction).[17] However, it becomes an even more troubling experience when the data trail that we leave is collected and aggregated from a variety of different sources, both online and offline.[18] The aggregation of data is performed both by commercial and government agencies and can provide a wealth of detail regarding personal habits, preferences, relationships and social networks. It collapses the divides that all people create between different areas of their lives.[19] We perform different aspects of ourselves in different contexts – we tailor our behaviour for work differently than we do for home, or for our friends, and so on.[20] The aggregation of data represents a loss of control of our carefully managed identities, collapsing the boundaries between private and public personas.

---

14 See generally Whitfield Diffie and Susan Landau, 'Communications Surveillance: Privacy and Security at Risk' (2009) 52(11) *Communications of the ACM* 42, 47; Marwick, above n 10.

15 Diffie and Landau, above n 14; Marwick, above n 10.

16 A 'cookie' is a small piece of data which records and uses certain information regarding the user, such as authentication, transaction history or order details.

17 Edward W Felten, 'Declaration of Professor Edward W Felten', Submission in *American Civil Liberties Union v Office of the Director of National Intelligence*, 13-cv-03994 (WHP), 26 August 2013, 13–14. See also Omer Tene, 'What Google Knows: Privacy and Internet Search Engines' [2008] *Utah Law Review* 1433, 1442–9, 1458.

18 Edward W Felten, 'Declaration of Professor Edward W Felten', Submission in *American Civil Liberties Union v Office of the Director of National Intelligence*, 13-cv-03994 (WHP), 26 August 2013, 17 [48] (emphasis in original):

> Analysis of metadata on this scale can reveal the network of individuals with whom we communicate–commonly called a *social graph*. By building a social graph that maps all of an organization's telephone calls over time, one could obtain a set of contacts that includes a substantial portion of the group's membership, donors, political supporters, confidential sources, and so on. Analysis of the metadata belonging to these individual callers, by moving one 'hop' further out, could help to classify each one, eventually yielding a detailed breakdown of the organization's associational relationships.

19 danah boyd, 'Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence' (2008) 14 *Convergence: The International Journal of Research into New Media Technologies* 13, 18.

20 Ibid; Erving Goffman, *The Presentation of Self in Everyday Life* (Anchor Books, 1959).

Our personal information has become commercially valuable. We do not reap the monetary benefits of commercial exchange in any tangible way, but our data is bought and sold by companies which exist solely to trade in the traces we leave of ourselves. They sell to other commercial organisations and to governments. The aggregation and sharing of data is not something that is in the control of the person whose data it is. It not only represents a loss of control, but as Bossewitch and Sinnreich point out, it is almost impossible to reverse the process[21] – to suck back data, to have it removed from a record of you that has proliferated to the point where you will never know how many instances of that data exist.

A further aspect of the aggregation and sharing of data is that one person's data is aggregated with other peoples' data – often in large sets of anonymised data. Through a series of processes discussed below, a personal data profile comes to be based not just on that person, but also on 'people like that person' as identified through these large scale anonymised data sets.[22]

Surveilling people's personally generated data without their knowledge also raises ethical concerns about the threat to intellectual freedom and privacy: how it 'affects the power balance between individuals and those who are watching', and the risks of 'harmful uses of sensitive information'.[23]

C Interrogation

A key aspect of this accumulation of data from multiple sources over long periods of time is that the data sets become so large as to be unmanageable. The 'infoglut' is beyond the comprehension of a single person.[24] The interrogation of the data at this scale is done rather by machines and algorithms.[25] This is not to say that people are not involved in the process of interrogation – people are responsible for writing the algorithms initially, for setting up the database categories that define how to think about what is important and what is not (a form of knowledge creation) and for 'cleaning up' the data to make it ready for the database.[26] Thus understanding the large datasets becomes the domain of those who create the algorithms. And algorithms themselves perform the task of pattern recognition on those data sets. How we become known through this

21 Jonah Bossewitch and Aram Sinnreich, 'The End of Forgetting: Strategic Agency beyond the Panopticon' (2012) 15 *New Media & Society* 224, 226.

22 Tene, above n 17, 1458.

23 Richards, above n 1, 1945. Further discussion of these issues: at 1945–58.

24 See Mark Andrejevic, *Infoglut: How Too Much Information Is Changing the Way We Think and Know* (Routledge, 2013).

25 Tarleton Gillespie, 'The Relevance of Algorithms' in Tarleton Gillespie, Pablo J Boczkowski and Kirsten A Foot (eds), *Media Technologies: Essays on Communication, Materiality, and Society* (MIT Press, 2014) 167.

26 See ibid 169–72.

process, how a personal profile of 'sufficient accuracy'[27] is generated, is to some extent based on the 'tyranny of the pattern'.[28]

More interesting still, from the point of view of regulation, is that algorithms can be programmed to 'learn' as they go. Machine based learning means that while a programmer may write the initial algorithm to interrogate the data, the algorithm then develops quite free from human intervention, creating its own investigations based on the patterns it recognises within the big data sets. Thus one person's profile is arrived at through processes of interrogation opaque even to the programmer.[29]

The data profiles (which are dynamic rather than static, as the accumulation and interrogation of data never stops) will never be a direct correlation to our 'real' selves. Decisions that we make that have been captured in data form can be de-contextualised and misinterpreted, motivations for particular actions are never explained or understood by the recording of them, and various things about us still escape capture. But this is not the only reason our profiles may be erroneous or misleading. Our profiles are often the result (as mentioned above) of the aggregation of our data with other peoples' data. We have been recognised through algorithms as being 'like' a variety of other people, and those peoples' choices and behaviours are absorbed into our profile as we are absorbed into theirs.[30] Furthermore, as Braman points out, there are practices designed to *protect* peoples' privacy, for example wherein aspects of their data are deliberately falsified before being shared in order to make the data more anonymous.[31] However, in the process of re-identification, which often is performed in a different context, such falsifications are not known or addressed. Our records have been tainted deliberately (ironically for our protection) but it is almost impossible to redress this misinformation downstream, where our loss of control of our data is almost complete.

An Australian Communications and Media Authority ('ACMA') report on how Australians manage their digital identities also noted that people deliberately falsify information about themselves as a privacy protection measure.[32] Their research found that 47 per cent of the Australians surveyed deliberately provided false or misleading information about themselves as a form of 'defensive inaccuracy'.[33] Where information is demanded by a website in order to gain access to that site and its services, people often choose to lie in an effort to

27 Ibid 174.

28 See Nimrod Kozlovski, 'Designing Accountable Online Policing' in Jack M Balkin et al (eds), *Cybercrime: Digital Cops in a Networked Environment* (New York University Press, 2007) 107, 115, discussing the 'tyranny of patterns' over accuracy.

29 See Gillespie, above n 25, 172.

30 Richards, above n 1, 1939.

31 Sandra Braman, 'Tactical Memory: The Politics of Openness in the Construction of Memory' (2006) 11(7) *First Monday* <http://firstmonday.org/ojs/index.php/fm/article/view/1363/1282>.

32 ACMA (Cth), *Managing Your Digital Identity: Digital Footprints and Identities Research Short Report 1* (2013) 6–8.

33 Ibid 6–7.

protect their identities. Thus that information, which is pulled into the data stream, will also feed into inaccuracies in a person's data profile that may or may not be damaging once that data is put to use in different contexts (say for credit applications, housing applications, or criminal profiling). Algorithms find patterns; they do not ask questions about the meaning of data or why particular choices are made by people.[34]

D Prediction

The uses made of data profiles that have been constructed through the above practices are consequently of great importance. Commercial uses such as selling profiles to advertisers are well established and in some ways can be seen as an extension of the practice of selling media audiences to advertisers which has sustained media businesses for many decades. The difference now is the more finely granulated targeting of advertisements to individuals. The sharing of profiles with government agencies, particularly security agencies is more controversial. It can be seen as a way for security agencies to circumvent the accountability and transparency mechanisms in place for the surveillance of citizens by 'outsourcing' the collection of data to commercial organisations, which also are often global in their reach and can ignore jurisdictional boundaries that restrict government activities.[35] The state thus has a vested interest in bolstering the power of corporations to gather information. While European data protection laws may attempt greater constraints on corporate data collection and storage,[36] the US government takes a very different stance toward regulating corporate practices. The revelations by Edward Snowden of the National Security Agency ('NSA') programs in 2013 involving big data give ample explanation as to how and why this stance is taken, as discussed below.

Of equal importance though, is the turn to prediction as a key mode of operation.[37] What big data offers both commercial and governmental organisations therefore is the seduction of predicting the future through the pattern recognitions offered by the algorithms interrogating the data: '[t]he promise of predictive analytics is to incorporate the future as a set of anticipated data points into the decision-making process'.[38]

---

34 See Andrejevic, above n 24, 1–41.

35 See, eg, Michael D Birnhack and Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8(6) *Virginia Journal of Law and Technology* 1, 17 [41].

36 See, eg, Tene, above n 17, 1437, 1459–60. See further discussion below.

37 See, eg, Edward W Felten, 'Declaration of Professor Edward W Felten', Submission in *American Civil Liberties Union v Office of the Director of National Intelligence*, 13-cv-03994 (WHP), 26 August 2013, 20–1 [61] (citations omitted):

> Researchers have discovered that individuals have unique calling patterns, regardless of which telephone they are using, they have figured out how to predict the kind of device that is making the calls (a telephone or a fax machine), developed algorithms capable of predicting whether the phone line is used by a business or for personal use, identified callers by social group (workers, commuters, and students) based on their calling patterns, and even estimated the personality traits of individual subscribers.

38 See Andrejevic, above n 24, 29.

Here we see the boundary between reality and simulation being crossed and recrossed as data is de-identified, aggregated, and interrogated by algorithms searching for patterns that might not otherwise have been noticed by human inquiry. Data is then reassembled into profiles that, while they *look* like a complete picture of someone, actually represent the aggregation of data from both that person and people the algorithms identify as like that person. Many aspects of data about that person may be left out, but predictions are made nonetheless, about their future behaviour.[39] What is interesting and worrying about this process is that the constitution of such profiles is opaque.

Pattern recognition is about correlations rather than causal relations. Algorithms notice correlations in data fragments without ever attempting to contextualise or explain.[40] They might notice for instance, that men who buy Schick razors are more likely to vote Republican, but they will not be able to provide an explanation. Thus if you are a man buying a Schick razor, the algorithm might predict that you also vote Republican. This is not based on any real understanding of you and your actions and motivations.

What needs to be understood is that this system of profiling and prediction is dynamic. As the data gathered is constantly updating, the algorithms may, upon the input of further data, find this correlation no longer holds (it does not care why), and so at a different point in time, will not predict that, as a Schick-buying man, you will vote Republican. Thus the predictions are always based on snapshots in time that could not be described as stable.[41] While this may not be a big issue in relation to marketing and the harms to an individual in their life as a consumer, it definitely takes on a problematic flavour if we consider criminal profiling or terrorist profiling.[42] If an algorithm, based on pattern recognition, constructs a profile of a person based not only on their own actions but the data gathered from other people whom the algorithm has determined are like that person (due to the choices it attributes to each), and at a given point in time, assesses that person as likely to commit a criminal act, or likely to be a terrorist, it may, sometime later, and with additional data, change its categorisation. As Amoore suggests, a profile could send up a flag one day but not the next.[43] The algorithms may, upon further calculations, take that person out of the category of likely criminal/terrorist. The predictions are not based on what will really happen. They are predictions, not facts. And yet, security agencies seeking to *prevent* acts, rather than address or respond to *actual* events, may well be seduced into treating these profiles and predictions as real. And if a person happens to be targeted through profiling based on a moment when they were

39 Richards, above n 1, 1957, discussing use of consumer data by Target stores.

40 Gillespie, above n 25, 174.

41 See, eg, John Cheney-Lippold, 'A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control' (2011) 28(6) *Theory, Culture & Society* 164, 169–70.

42 See, eg, Louise Amoore, 'Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times' (2011) 28(6) *Theory, Culture & Society* 24, 32.

43 Ibid.

algorithmically predicted to belong to a category, it will be very difficult to find some form of redress. Using machine generated calculations means that even the people who write the algorithms do not really know what the algorithm was recognising and aggregating at the moment in time when it categorised a person. The algorithm will likely have morphed into something different by the time redress is sought.[44]

If we consider what it might take to challenge inaccuracies in a data profile – particularly if that profile has been used in a way that is detrimental to a person – the process is not the same as challenging inaccuracies of data kept about a person's *actual* life actions. That would be about the data collection (and possibly archiving) on a person. As Crawford and Schulz suggest, there needs to be a means to 'audit the data that was *used* to make a determination' on someone,[45] which means data from a range of sources, not all of them from the actual person. A decision based on a data profile is a decision based on predictions derived from that person and many other people as well. The data profile represents many different categorisations that have been made across a range of data. Predictive algorithms, having found patterns across large sets of data, and having determined correlations that may or may not hold, might categorise a person without any regard to their actual behaviour, but more on who the algorithm predicts they are.[46] But as Andrejevic points out, although people are behind the process of deciding what is important to notice and what can be ignored at some point, the algorithms are also programmed to learn, machinically, and transform as they proceed.[47] Thus the chances of transparency and accountability become exceedingly remote as even the programmers who write the algorithms lose track of what those algorithms are actually calculating and interrogating.

II CHALLENGES CREATED BY CURRENT DATA PRACTICES

From this brief overview of some aspects of current data collection and usage practices it can be seen that regulation of this area is a difficult challenge. Privacy regulation through privacy statutes, common law and data protection laws links an individual to their records, protecting the records in order to protect the interests of the related individual. Big data seemingly severs the individual from

44 Gillespie, above n 25, 172.

45 Discussing 'data due process': Kate Crawford and Jason Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55 *Boston College Law Review* 93, 117. See also Sara M Watson, 'Data Doppelgängers and the Uncanny Valley of Personalization', *The Atlantic* (online), 16 June 2014 <http://www.theatlantic.com/technology/archive/2014/06/data-doppelgangers-and-the-uncanny-valley-of-personalization/372780/>: 'We need to demand more ways to keep our data doppelgängers in check.'

46 See Gillespie, above n 25, 173–4.

47 See Andrejevic, above n 24, 1–41.

their data, thus removing the justifications for protection under traditional concepts of privacy. However, the mass collection of seemingly de-identified data may in fact now result in the generation of more detailed and more accurate profiles of a larger number of individuals than more targeted surveillance of the individuals could produce.[48] The impact of the collection and use of metadata must therefore be assessed through a different lens.

Privacy regulation in Australia deals primarily with restricting the collection, use of and access to particular categories of information about a person by the public, government or corporations.[49] But in the space of big data, many of the fixed boundaries around information that are part of how privacy regulation can structure a regulatory system using gates and walls, are simply not found. Algorithms voraciously travel across many boundaries. The processes involved in data analytics, predictive analytics and the creation of data profiles tend to exceed the forms and assumptions of privacy regulation. Algorithms may create new categories on the fly, thus exceeding regulatory mechanisms that attempt to quarantine content from use through categories.[50] The idea of consent becomes unworkable in an environment where it is not known, even by the people collecting and selling data, what will happen to the data – one cannot give meaningful consent to an unknown use of data downstream in the process.[51] Further, the notion of consent is compromised where the user must consent to disclose certain personal data in order to use (increasingly ubiquitous) services such as apps, social media, search engines, or email. For example, internet radio app Pandora now claims that an algorithm based on its subscribers' voluntarily disclosed music preferences and election results enables it to predict users' voting preferences with great accuracy.[52] Pandora users are required to disclose

48 See generally Edward W Felten, 'Declaration of Professor Edward W Felten', Submission in *American Civil Liberties Union v Office of the Director of National Intelligence*, 13-cv-03994 (WHP), 26 August 2013, 22 [64]:

> The privacy impact of collecting all communications metadata about a single person for long periods of time is qualitatively different than doing so over a period of days. Similarly, the privacy impact of assembling the call records of every American is vastly greater than the impact of collecting data about a single person or even groups of people. Mass collection not only allows the government to learn information about more people, but it also enables the government to learn new, previously private facts that it could not have learned simply by collecting the information about a few, specific individuals.

49 See generally *Privacy Act 1988* (Cth). This relates to personal information disclosed by individuals or collected about the individual for the purposes of transacting with that agency, department, business or company in some way. It would not apply to calculations or algorithmic assumptions based on anonymous data. Similar limitations apply in privacy laws in the UK and US, see: *Human Rights Act 1998* (UK) c 42, sch 1 art 8; *Stored Communications Act,* 18 USC §§2701–12 (1986); *Electronic Communications Privacy Act of 1986*, 18 USC §§2510–22.

50 Crawford and Schultz, above n 45, 106.

51 See, eg, Solove, above n 11, 1881.

52 Elizabeth Dwoskin, 'Pandora Thinks It Knows if You Are a Republican', *The Wall Street Journal* (online), 13 February 2014 <http://online.wsj.com/news/articles/SB10001424052702304315004579381393567130078>.

personal preferences and information in order to facilitate targeted advertising and thus subscribe to the 'free' service.

Solove points out that regulation based on consent is ineffective when, as is the case with data gathering currently, the scale of the exercise is unmanageable, the downstream uses are difficult to assess, and assessing harm is also difficult when harm can be cumulative,[53] and social rather than individual (for instance in the case of racial profiling). One cannot seek to have the record corrected if the data identified as incorrect has been proliferated across an unknown number of nodes of the network and may be working in any number of profiles – both of the person and of other people.[54] The proliferation of sites where data about a person are held, and the possibilities of it being archived over and over make the idea of redress on this level an impossibility. Ironically, as Amoore points out, algorithms do not need to archive data or store it.[55] They are the calculating processes that look at data and move on – making associative connections and changing constantly in iterative processes that suggest constant dynamism – rather than fixity and static categories that can be grasped and controlled by regulatory mechanisms of the kind seen in current privacy regimes. Crawford and Schulz suggest that rather than attempting to erect walls around categories (which algorithms will change or discard anyway) the idea of regulation must instead focus on the *processes* involved in establishing algorithms and the use of the resulting conclusions.[56] Although this notion of due process, the right to correct the record, and proper disclosure of both the use of predictive data derivatives and disclosure of the sources those predictions are based upon, seems more plausible than focusing on content, in reality even these measures of procedural fairness would be difficult to implement.

Focussing on processes and uses of both personally identifiable information *and* predictive data represents a shift away from privacy protection frameworks designed to restrict the capture and storage of data, and limit access and uses based on content categories. These mechanisms seem to be no longer adequate or appropriate, although the desire for accountability and transparency remain. The intersection of the discourses of privacy with those of security and risk ensure that governments find themselves with internal conflicts of interest. Attempts to minimise risk and to enhance security are often in conflict with obligations to ensure the privacy of citizens,[57] and many governments seem reluctant to restrict the former in favour of the latter. As Dean points out, the encroachments of the

53 Solove, above n 11, 1888–90, 1892.
54 See generally Bossewitch and Sinnreich, above n 21, 226.
55 Amoore, above n 42, 33.
56 Crawford and Schultz, above n 45, 106, 109.
57 See Sal Humphreys, 'Predicting, Securing and Shaping the Future: Mechanisms of Governance in Online Social Environments' (2013) 9 *International Journal of Media and Cultural Politics* 247, 252–5.

security arm of government through the normalisation of 'crisis' situations requiring the overriding of citizen privacy rights is now well established.[58]

We will now turn to the specific legal issues which have recently been litigated in the US and UK concerning big data.

III LEGAL RESPONSES: US AND UK EXPERIENCES

A Metadata Capture: Section 215 Program and PRISM

The issue of privacy, surveillance and mass data capture came to the forefront in June 2013 with the revelations by former NSA contractor Edward Snowden that the US government, through its various agencies, was engaging in massive scale collection of data from both its own and foreign citizens.[59] This data collection was occurring in the context of two separate but similar programs: the first, known as the 'section 215 program' facilitated the collection of telephony metadata, capturing caller ID, numbers dialed, place of call, duration and other information, but not including the content of the call. One of Snowden's first leaks revealed that Verizon, a major US telecommunications provider, was compelled by order of the Foreign Intelligence Surveillance Court ('FISC')[60] to produce to the NSA daily records of all telephony metadata for communication between the US and abroad and wholly within the US, including local telephone calls.[61] In response to these disclosures the US government confirmed that such a program did in fact exist, pursuant to which 'the FBI obtains orders from the FISC pursuant to Section 215 [of the *USA PATRIOT Act*][62] directing certain telecommunications service providers to produce to the

58 Mitchell Dean, 'Power at the Heart of the Present: Exception, Risk and Sovereignty' (2010) 13 *European Journal of Cultural Studies* 459, 464.

59 For a detailed insight into these disclosures and Snowden's actions and motivations, see Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (Penguin Books, 2014).

60 The FISC, established under the provisions of the *Foreign Intelligence Surveillance Act*, 50 USC §§ 1801–85 (1978) ('*FISA*'), hears ex parte applications from the US government to authorise domestic electronic surveillance for foreign intelligence purposes. The judges are drawn from the ranks of District Court and the matters are heard in secret, with no public records of proceedings. In the period since 1978 the Court has approved over 20 000 requests and rejected only a handful. As Greenwald notes, its role appears to be more as a 'part of the executive branch rather than as an independent judiciary exercising real oversight': ibid 128.

61 Glenn Greenwald, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily', *The Guardian* (online), 6 June 2013 <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>. It was quickly revealed that other phone providers were also subject to such orders.

62 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, 50 USC § 1861 ('*USA PATRIOT Act*').

NSA on a daily basis electronic copies of "call detail records."'[63] The second of Snowden's leaks detailed the collection of online user data from major US technology companies such as Google and Apple, by the government as part of a program known as 'PRISM'.[64] We can see here the ability of governments to 'outsource' the collection of data to private corporations whose data collection crosses jurisdictional boundaries with impunity. Again the US government confirmed the existence of such a program, but claimed that it was targeted only at non-US citizens, and was authorised under the *FISA*.[65]

Both the section 215 and PRISM programs are designed around the fact that different legal frameworks apply in the US with respect to surveillance of 'foreign' and 'domestic' persons.[66] Any surveillance of a US person must comply with constitutional and legal requirements, notably obtaining a warrant. However, legal restrictions upon surveillance without a warrant do not apply to non-US persons located outside of the US. Thus two very different surveillance frameworks exist in theory, but with global networks of communication and the centrality of the US to the global internet and communication industries, these boundaries appear to have become very blurred. US citizens were appalled that their constitutional rights under the Fourth Amendment[67] appeared to have been violated.

Well before Snowden's revelations, there had been concerns expressed regarding the data gathering activities of the NSA. In February 2013, the US Supreme Court handed down its decision regarding a group of lawyers, non-governmental organisations ('NGOs'), human rights, labour, and media organisations who sought a declaration that section 1881a of the *FISA* was unconstitutional,[68] and a permanent injunction against section 1881a-authorised

---

63 *Klayman v Obama*, 957 F Supp 2d 1, 10 (D DC, 2013). The case notes the various public statements made by the Office of the Director of National Intelligence following Snowden's disclosures: at 10 n 9. See, eg, James R Clapper, Director of National Intelligence, 'DNI Statement on Recent Unauthorized Disclosures of Classified Information' (Press Release, 6 June 2013) <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information?tmpl=component&format=pdf>.

64 Glenn Greenwald and Ewen MacAskill, 'NSA Prism Program Taps in to User Data of Apple, Google and Others', *The Guardian* (online), 7 June 2013 <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

65 *FISA* § 1881a; Dan Roberts, Spencer Ackerman and Tania Branigan, 'Clapper Admits Secret NSA Surveillance Program to Access User Data', *The Guardian* (online), 8 June 2013 <http://www.theguardian.com/world/2013/jun/07/clapper-secret-nsa-surveillance-prism>.

66 *USA PATRIOT Act*, 50 USC §§ 1861, 1881 (2001).

67 *United States Constitution* amend IV. It establishes:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

68 *Clapper v Amnesty International USA*, 133 S Ct 1138, 1142 (Alito J). The respondents argued that § 1881 violated the Fourth and First Amendments, art III of the *Constitution* and the separation of powers principles: at 7 [C].

surveillance.[69] The respondents claimed that their work required them to 'engage in sensitive and sometimes privileged communications' via 'telephone and email with their clients, colleagues, sources' and 'other' relevant parties who may be located outside of the US.[70] They claimed that some of the people with whom they exchanged information were likely to be targets of surveillance under section 1881a, including those 'people the Government "believes or believed to be associated with terrorist organizations," "people located in geographic areas that are a special focus" of the Government's counterterrorism or diplomatic effort, and activists who oppose governments that are supported by the United States Government.'[71] The threat of surveillance compromised their ability to communicate with their clients and other important sources, chilled their ability to communicate and required additional measures to protect the confidentiality of their communications, including travelling overseas to meet face to face, and other measures.[72]

Section 1881a authorises the US Attorney-General and the Director of National Intelligence to 'acquire foreign intelligence information by jointly authorising the surveillance of individuals who are not 'United States persons' and are reasonably believed to be located outside of the US'.[73] Normally, the approval of the FISC is also required and, as the Supreme Court observed, surveillance is subject to 'statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment.'[74] The case revolved around the question of standing, whether the respondents could establish injury in fact based on their claim that there was a strong likelihood that their communications would be acquired under section 1881a in the future thus causing them injury, or alternatively that they were sustaining injury as a consequence of the fact that the risk of section 1881a-authorised surveillance was requiring them to take 'costly and burdensome measures to protect the confidentiality of their international communications.'[75] The Supreme Court held that the respondents lacked the requisite standing on the basis that they had no actual knowledge of the government's targeting practices under section 1881a and that claims of fears of widespread surveillance of the communications were merely speculative.[76] Further, the Court held the respondents could not establish that the interception may be authorised under some other provision of FISA, nor

69 Section 1881a was added to *FISA* by the *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008* Pub L No 110–261, 122 Stat 2436 (2008).

70 *Clapper v Amnesty International USA*, 133 S Ct 1138, 1145 (Alito J).

71 Ibid, quoting App. to Pet. for Cert. 399a.

72 *Clapper v Amnesty International USA*, 133 S Ct 1138, 1145–6 (Alito J).

73 *FISA* §1801(i) states that 'United States person' includes US citizens, aliens admitted for permanent residence and certain associations and corporations.

74 *Clapper v Amnesty International USA*, 133 S Ct 1138, 1144 (Alito J).

75 Ibid 1143 (Alito J).

76 Ibid 1143, 1148–50. Eg, the Court cites journalist Christopher Hedges: 'I have no choice but to assume that any of my international communications may be subject to government surveillance, and I have to make decisions … in light of that assumption': at 1148 (Alito J).

could they demonstrate that even if the government sought to invoke surveillance of communications with their foreign contacts 'that the FISC would authorise such surveillance', that the communications could actually be acquired nor that their own communications would be caught up in such surveillance.[77] Any costs incurred by the respondents in attempting to avoid surveillance were based on their own 'fears of hypothetical future harm that is not certainly impending.'[78]

Justice Breyer filed a dissenting opinion, which concluded that, based on the nature of the communications engaged in by the respondents, the past conduct of the government and the capacity to undertake the surveillance, there 'is a high probability that the Government will intercept at least some electronic communication to which at least some of the plaintiffs are parties.'[79] It was therefore wrong to characterise the harm threatened to the respondents as 'speculative' and 'at least some' of the respondents were entitled to standing.[80]

Of course, just how 'speculative' these claims were was revealed with dramatic consequences only a few months later when the government was forced by Snowden's revelations to confirm its existence and consider how it could combat the massive anger of its own and foreign citizens, and the consequent collateral damage it had inflicted on its own technology industry. What had been merely speculative in February was confirmed as widespread practice in June.

B US Government Responses

The surveillance practices of the US government outlined above were reviewed in the *Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies: Liberty and Security in a Changing World*,[81] commissioned by President Obama in August 2013 and released in December 2013. The report was commissioned in response to public and global pressure brought to bear on the US President regarding how he would respond to the Snowden revelations, which were having serious fallout for the US worldwide. However, in addition to the section 215 program and PRISM revelations, further disclosures continued to flow from Snowden. Not only was the US now implicated in spying on governments of hostile nations, it had been caught tapping the phone of German Chancellor Angela Merkel.[82] Further, several governments allied with the US, including the UK and Australia, were

77 Ibid 1141 (Alito J).
78 Ibid 1151 (Alito J).
79 Ibid 1160.
80 Ibid.
81 President's Review Group on Intelligence and Communications Technologies, Office of the Director of National Intelligence (US), *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* (2013) ('*Liberty and Security Report*').
82 Ian Traynor, 'Angela Merkel: NSA Spying on Allies Is Not On', *The Guardian* (online), 25 October 2013 <http://www.theguardian.com/world/2013/oct/24/angela-merkel-nsa-spying-allies-not-on>.

implicated in mass surveillance practices, including spying on one another's citizens.[83]

The fact that US technology companies had been the instrument of widespread user surveillance also generated massive user backlash and a commercial headache for these companies who depend heavily upon user trust. The Obama regime was forced into damage control.

The *Liberty and Security Report* identified a number of principles which should underpin intelligence collection activities into the future.

'1. The United States Government must protect, at once, two different forms of security: national security and personal privacy.'[84] This statement highlights the dualistic nature of the concept of 'security', reflecting both the concepts of national security and defence against enemies of the United States,[85] and the articulation in the Fourth Amendment of the right of the people of the United States 'to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures'.[86] This notion of security has created significant conceptual problems in defining the scope of the right of privacy. As Wacks has observed, the inclusion of security against unreasonable searches and seizures in the Fourth Amendment has manifested in the grafting of notions of personal autonomy onto the concept of personal privacy.[87] According to Wacks, this lack of conceptual clarity, contained within the original Warren and Brandeis thesis on privacy, was further complicated by Prosser's gloss, which added concepts of personal freedoms, including speech and personal autonomy, to concepts of confidentiality.[88] Justice Brandeis equated this right of privacy to both the 'the right to be let alone' and to the essential right of self-fulfilment, as the capacity to fully and freely express one's thoughts and emotions are a vital part of an individual's pursuit of happiness.[89] As Wacks points out, this conflates two entirely different concepts: confidentiality and autonomy.[90] Therefore, there are tensions within the very concept of privacy as well as in the various roles it is expected to perform. Thus the wording of the Fourth Amendment complicates the concept of privacy, posing significant difficulties in articulating a clear, meaningful and legally enforceable concept of 'privacy'.

---

83 Bernard Keane, 'Spy versus Spy; Gatekeeper versus Gatekeeper', *Crikey* (online), 22 November 2013 <http://www.crikey.com.au/2013/11/22/spy-versus-spy-gatekeeper-versus-gatekeeper/>.

84 *Liberty and Security Report*, above n 81, 14.

85 Ibid 15.

86 Ibid.

87 Raymond Wacks, *Privacy and Media Freedom* (Oxford University Press, 2013) 55.

88 Ibid 55–9. See also Samuel V Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 98 *Harvard Law Review* 193; William L Prosser, 'Privacy' (1960) 48 *California Law Review* 383; Neil Richards and Daniel Solove, 'Prosser's Privacy Law: A Mixed Legacy' (2010) 98 *California Law Review* 1887.

89 *Olmstead v United States*, 277 US 438, 478 (Brandeis J) (1928).

90 The identification of these concepts in terms of 'security' also gives rise to tension between national security interests and personal privacy, as has recently been recognised in the *Liberty and Security Report*, above n 81, 43–6. See also Wacks, above n 87.

'2. The central task is one of risk management; multiple risks are involved, and all of them must be considered.'[91] In addition to the obvious question of risks to national security, public officials should consider 'risks to privacy', 'risks to freedom and civil liberties, on the Internet and elsewhere', risks to the relationships of the US with other nations, and 'risks to trade and commerce, including international commerce.'[92] These 'other' risks, it could be argued, were overlooked (or overridden) by the section 215 and PRISM collection programs. It appears to be a case of the practical fact that such data *can* be collected and therefore it *should* be collected.

'3. The idea of "balancing" has an important element of truth, but it is also inadequate and misleading.'[93] The determination of the correct nature of the scope of surveillance could not be determined by a simple balancing exercise between the two identified forms of security (national and personal).[94] In fact, some other relevant considerations are also subject to this balancing exercise, such as: surveillance should not be conducted in order to

> punish … political enemies; to restrict freedom of speech or religion; to suppress legitimate criticism and dissent; to help … preferred companies or industries; to provide domestic companies with an unfair competitive advantage; or to benefit or burden members of groups defined in terms of religion, ethnicity, race and gender.[95]

'4. The government should base its decisions on a careful analysis of consequences, including both benefits and costs (to the extent feasible).'[96] Application of this final principle appears absent from the implementation, operation and continuation of the section 215 and PRISM programs. There is a clear reluctance to forego the access to data which may be relevant to a security risk or criminal investigation. Rather than seek a warrant for relevant data as a need arises, all data is captured in the belief of its potential usefulness, and as noted above, the capture of this mass data set then facilitates downstream unanticipated (and potentially uncontrolled) uses. Further, studies have confirmed that far from consisting of unidentified snippets of non-personal data, telephony metadata 'can be extremely revealing, both at the level of individual calls and, especially, in the aggregate.'[97] The metadata is easily searchable and can reveal details regarding an individual's personal circumstances, location, political, religious and sexual preferences and relationships with others.

---

91 *Liberty Security Report*, above n 81, 15.
92 Ibid.
93 Ibid 16.
94 Ibid.
95 Ibid.
96 Ibid.
97 Edward W Felten, 'Declaration of Professor Edward W Felten', Submission in *American Civil Liberties Union v Office of the Director of National Intelligence*, 13-cv-03994 (WHP), 26 August 2013, 13 [38]. See also Jonathan Mayer and Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata* (12 March 2014) Web Policy <http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/>.

The Report's 46 recommendations reflect the extensive damage inflicted on US government and business interests by the Snowden revelations. A number of the key recommendations will be highlighted here.

Unsurprisingly, the Report does not recommend the abolition of surveillance and intelligence gathering activities. Rather, the Report begins with the acknowledgement that the US 'must continue to collect signals intelligence globally in order to assure the safety of [US] citizens at home and abroad and to help protect the safety of our friends, our allies, and the many nations with whom we have cooperative relationships.'[98] However, it does recommend the end of bulk storage of data under section 215 of *FISA* and that metadata should be transferred to a private provider who would store such data for interrogation by the government as appropriate for national security purposes.[99] Further, telephone, internet and other service providers should be able to publicly disclose general information about orders they receive requiring them to provide information to the government, such as the number of requests received, categories of information provided and the numbers of users involved.[100] Safeguards need to be put in place to ensure that the collection of information from non-US persons is subject to additional safeguards, including prohibitions on obtaining information for commercial gain for domestic industries.[101]

The Report examines in detail the question of what privacy interests are implicated by the mass collection of metadata from phone and internet records of individuals and businesses.[102] Noting that the Fourth Amendment had been interpreted by the US Supreme Court in a series of decisions in the 1970s to

---

98 *Liberty and Security Report*, above n 81, 11.

99 Ibid 25. Recommendation 4 suggests:

> as a general rule, and without senior policy review, the government should not be permitted to collect and store all mass, undigested, non-public personal information about individuals to enable future queries and data-mining for foreign intelligence purposes. Any program involving government collection or storage of such data must be narrowly tailored to serve an important government interest.

Further, Recommendation 5 suggests 'legislation should be enacted that terminates the storage of bulk telephony meta-data by the government under section 215, and transitions as soon as reasonably possible to a system in which such meta-data is held instead either by private providers or by a private third party.'

100 See Recommendation 9: ibid 27.

101 The US Government should affirm that surveillance of non-US persons outside of the US:

> (1) must be authorized by duly enacted laws or properly authorized executive orders;
> (2) must be directed *exclusively* at the national security of the United States or our allies;
> (3) must *not* be directed at illicit or illegitimate ends, such as the theft of trade secrets or obtaining commercial gain for domestic industries; and
> (4) must not disseminate information about non-United States persons if the information is not relevant to protecting the national security of the United States or our allies.
>
> In addition, the US Government should make clear that such surveillance:
>
> (1) must not target any non-United States person located outside of the United States based solely on that person's political views or religious convictions; and
> (2) must be subject to careful oversight and to the highest degree of transparency consistent with protecting the national security of the United States and our allies.

See Recommendation 13: ibid 29–30 (emphasis in original).

102 *Liberty and Security Report*, above n 81, 11, chs III–IV.

allow collection of information voluntarily shared with third parties, the Report observes the possible emergence of a need to reconsider the approach that individuals have no 'reasonable expectation of privacy' in this information (whilst observing that it is not the role of the Report to interpret the Fourth Amendment in this context, leaving that decision to the Supreme Court).[103] The continuing validity and scope of application of this line of authority in the digital era was raised but not resolved in *United States v Jones*,[104] which concerned the constitutionality of the surveillance of an individual suspected of drug trafficking, by attaching a GPS to his car. The Court concluded (by majority) that the installation of the GPS was a 'search' within the meaning of the Fourth Amendment, but declined to further consider the argument that such surveillance was legitimate based on the argument that an individual's movements along public roads are voluntarily disclosed to third parties in accordance with the logic of *Miller* and *Smith*.[105] Thus until *Miller* and *Smith* are reviewed by the Supreme Court, they remain good law, and create a low threshold test regarding privacy of individual information.

The Report acknowledges that the bulk collection of undigested, non-public personal information about individuals involves serious implications of invasions of privacy. Essentially people must reveal personal information to banks, phone companies, health providers and so on in order to participate in modern society, so the question of whether the person has voluntarily decided to reveal such information is moot.[106] Notably this discussion leaves aside any related questions regarding the status of disclosures made to social networking sites, now used as a major conduit of communication. Further, there is a real concern that people are becoming increasingly aware of the fact that their personal information is being monitored, collated and used and therefore may be prevented from fully participating in society as a consequence, contrary to the purposes of the Fourth and First Amendments.[107]

The Report notes the damage that can potentially be caused by aggressive surveillance practices not only to US businesses, but further to the future

---

103 See *Miller v United States*, 425 US 435 (1976) ('*Miller*') (bank records) and *Smith v Maryland*, 442 US 735 (1979) ('*Smith*') (telephone records). The Report notes that these decisions underpin the enactment of s 215 of the *USA PATRIOT Act*, which authorises the making of orders compelling the production of a large variety of records under *FISA*: *Liberty and Security Report*, above n 81, 83–4.

104 132 S Ct 945 (2012).

105 See ibid 957 (Sotomayor J). Eg, Sotomayor J observed:

> it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties … This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. … I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

See generally *Liberty and Security Report*, above n 81, 84–5.

106 *Liberty and Security Report*, above n 81, 111–12.

107 Ibid 110–12, quoting National Research Council of the National Academy of Science, *Protecting Individual Privacy in the Struggle against Terrorists: A Framework for Program Assessment* (National Academic Press, 2008) 2–3.

openness of the internet, and even democracy itself.[108] It highlights the large losses caused to US cloud computing providers due to concerns regarding their implication in US surveillance, harming US economic growth.[109]

Further, the US agenda regarding internet freedom has been seriously undermined by the revelations. Not only does this create the potential for harm to US internet business interests, but also sustains calls for closed and localised internet models contrary to US policy on the future of the global internet.[110]

The concern regarding harm to US internet and technology companies is not overstated. Snowden's leaked documents included a PowerPoint presentation prepared for the NSA identifying by name and logo the technology companies, including Microsoft, Yahoo, Google, Facebook and Apple, that participated in the PRISM program (this following immediately upon similar revelation regarding telephone companies).[111] The companies issued denials regarding their involvement in the mass collection of data, but they could not deny that they had been compelled to provide records to the US Government.[112] They had not however been allowed to reveal their involvement due to the fact they were prevented by a court order. This complicity with covert surveillance of global internet users threatened the very substance of the internet, undermining the characterisation of the internet and technology companies as the engine of free speech. Rather the internet could become 'a means of widespread surveillance'.[113] Businesses such as Google base their whole business model on asking their users to trust them with vast amounts of data, making them very attractive data sources. However, without that trust their businesses will shrink and possibly fail: imagine a Facebook or Instagram where people refuse to post any personal information.

The technology companies went into damage control mode issuing the Global Government Surveillance Reform statement calling for reform of government surveillance practices.[114] In particular, they claimed, collection of

108 'In light of the global influence of the United States, any threat to effective democracy in the United States could have negative and far-reaching consequences in other nations as well': *Liberty and Security Report*, above n 81, 154.

109 Ibid 212.

110 Ibid 213–15.

111 Steven Levy, *How the NSA Almost Killed the Internet* (7 January 2014) Wired <http://www.wired.com/threatlevel/2014/01/how-the-us-almost-killed-the-internet/all>.

112 Greenwald, above n 59, 108–18.

113 Levy, above n 111.

114 Reform Government Surveillance, *The Principles* (2014) <https://www.reformgovernmentsurveillance.com> ; Open Letter from AOL et al to the US President and Members of Congress, 9 December 2013 <https://www.reformgovernmentsurveillance.com/>. See also Steve Holland and Roberta Rampton, 'Tech Executives Press Barack Obama to Reform NSA Surveillance Practices', *The Sydney Morning Herald* (online), 18 December 2013 <http://www.smh.com.au/it-pro/security-it/tech-executives-press-barack-obama-to-reform-nsa-surveillance-practices-20131217-hv67u.html>; Dominic Rushe and Paul Lewis, 'Tech Firms Push Back against White House Efforts to Divert NSA Meeting', *The Guardian* (online), 18 December 2013 <http://www.theguardian.com/world/2013/dec/17/tech-firms-obama-meeting-nsa-surveillance>.

information should be transparent and sufficiently targeted. Governments should not 'undertake' or require 'bulk data collection of internet communications'.[115]

Recognising the potential for significant harms to US business interests, as well as the broader harm of the potential 'balkani[sation]' of the internet, President Obama released the Presidential Policy Directive on 17 January 2014.[116] Section 1 confirms that '[p]rivacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities.'[117] Signals intelligence may not be collected for other purposes, such as suppressing speech, nor to offer a competitive advantage to US businesses.[118] The Directive is clear on the point that collection of bulk data will continue. However, new limits are to be imposed on the use of that data. Data may be used for the purposes of detecting and countering: espionage and threats against the US from terrorism, spying and other activities, weapons of mass destruction, cybersecurity; threats to US and Allied armed forces and other personnel and transnational criminal threats.[119] At the same time, President Obama announced a number of other reforms, designed to increase accountability and transparency regarding the US government's surveillance activities, including some declassification of orders of the FISC, which provides review of the program targeting foreign individuals outside of the US and the section 215 telephony metadata program discussed above.[120] Further, the section 215 program will be replaced with a new procedure. Noting the recommendations of the Review Group that a third party rather than the government retains the bulk data, which may then be interrogated by the government on an as needs basis, President Obama reflected on the complexities generated by such an approach:

> Relying solely on the records of multiple providers, for example, could require companies to alter their procedures in ways that raise new privacy concerns. On the other hand, any third party maintaining a single, consolidated database would be carrying out what is essentially a government function but with more expense, more legal ambiguity, potentially less accountability -- all of which would have a doubtful impact on increasing public confidence that their privacy is being protected.[121]

These announcements were criticised as merely a publicity stunt in order to direct attention away from the harm being inflicted on the US technology

115 AOL et al, *The Principles* (2014) Reform Government Surveillance <https://www.reformgovernment surveillance.com/#>.

116 Office of the Press Secretary, 'Signals Intelligence Activities' (Presidential Policy Directive, PPD–28, 17 January 2014).

117 Ibid 2.

118 Ibid.

119 Ibid 3.

120 Barack Obama, 'Remarks by the President on Review of Signals Intelligence' (Speech delivered at the Department of Justice, Washington, D C, 17 January 2014) <http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>.

121 Ibid.

industry.[122] Indeed, little reform has been effected since January 2014. As noted above, bulk collection of telephony metadata by the NSA has ceased (although still conducted by third parties) but the USA Freedom Act,[123] intended to restrict the surveillance powers of the NSA with respect to the internet, has fallen victim to political maneuvering, despite significant lobbying from the US technology industries.[124] The revised Act passed the House in May 2014 with none of the safeguards against continued surveillance that had been anticipated.[125] Therefore mass data capture remains legal in the US.[126]

C US Judicial Responses

Of course, Snowden's revelations also demonstrated that the collection of data described by the Supreme Court as speculative, was in fact actually occurring, opening the door again for challenges to the constitutionality of such practices. By December 2013, two conflicting District Court decisions had been handed down on the question of standing to sue on the constitutionality of bulk collection of telephony metadata: *Klayman v Obama*,[127] and decision reached a different outcome. The plaintiffs in *Klayman* commenced two actions, one related to the capture of telephone data from Verizon, brought against the NSA, the Department of Justice, President Obama and several other executive officials, as well as Verizon ('*Klayman I*'), and the second with respect to the monitoring of internet services, brought against the same government defendants and Facebook, Yahoo!, Google, Microsoft, YouTube, AOL, PalTalk, Skype, Sprint, AT&T and Apple ('*Klayman II*'). Both claims alleged that the government violated the plaintiffs' rights under the First, Fourth and Fifth Amendments and the *Administrative Procedure Act* by exceeding its authority under *FISA*.[128] In *Klayman I* the Court held that the plaintiffs had 'standing to challenge the constitutionality of the Government's bulk collection and querying of phone record metadata, that they have demonstrated a substantial likelihood of success

122 Glenn Greenwald, 'Obama's NSA "Reforms" Are Little More than a PR Attempt to Mollify the Public', *The Guardian* (online), 18 January 2014 <http://www.theguardian.com/commentisfree/2014/jan/17/obama-nsa-reforms-bulk-surveillance-remains>.

123 HR 3361, 113th Congress (2013).

124 See, eg, Steve Wilson (ed), 'Mark Zuckerberg Tells Barack Obama He Is 'Frustrated' over US Government Surveillance', *The Telegraph* (online), 14 March 2014 <http://www.telegraph.co.uk/technology/mark-zuckerberg/10697059/Mark-Zuckerberg-tells-Barack-Obama-he-is-frustrated-over-US-government-surveillance.html>.

125 Spencer Ackerman, 'Edward Snowden, a Year On: Reformers Frustrated as NSA Preserves Its Power', *The Guardian* (online), 5 June 2014 <http://www.theguardian.com/world/2014/jun/05/edward-snowden-one-year-nsa-surveillance-reform>.

126 See ibid. However, the House of Representatives also recently voted to remove the power from the NSA to search 'warrantlessly through its troves of ostensibly foreign communications content for Americans' data, the so-called "backdoor search" provision': see Spencer Ackerman, 'House of Representatives Moves to Ban NSA's "Backdoor Search" Provision', *The Guardian* (online), 21 June 2014 <http://www.theguardian.com/world/2014/jun/20/house-bans-nsa-backdoor-search-surveillance>.

127 957 F Supp 2d 1 (D Colo, 2013).

128 *Klayman v Obama*, 957 F Supp 2d 1, 11 (Leon J) (D Colo, 2013).

on the merits of their Fourth Amendment claim, and that they will suffer irreparable harm absent preliminary injunctive relief.'[129] However, given the national security interests implicated in the case, the injunction would be stayed pending appeal.[130]

In *American Civil Liberties Union v Clapper*,[131] Pauley III DJ reached the opposite conclusion, finding that the bulk telephony metadata program is lawful and not susceptible to a constitutional challenge. Revisiting the claims that had been made in the earlier Supreme Court case of *Clapper v Amnesty International USA*, the American Civil Liberties Union ('ACLU') based its claim on three sources of injury:

1. the 'collection of … metadata related to the ACLU's phone calls';[132]
2. the search of the metadata related to the ACLU's phone calls when the NSA checks the phone numbers three 'hops' away from the 'seed' number (ie, the number which is the subject of the search); and
3. the chilling effect on all those who may hesitate to make contact with the ACLU due to knowledge that the NSA will have a record that such a telephone number was used to make that contact with the ACLU.[133]

In this case, however, the ACLU was granted standing on the basis that it was no longer in dispute that the government had collected the metadata relating to the ACLU's phone calls.[134] With respect to the argument under the Fourth Amendment, the ACLU argued that:

> analysis of bulk telephony metadata allows the creation of a rich mosaic: it can 'reveal a person's religion, political associations, use of a telephone-sex hotline, contemplation of suicide, addiction to gambling or drugs, experience with rape, grappling with sexuality, or support for particular political causes.[135]

The Court rejected this argument and noted that '[t]he collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search.'[136] Declaring that the Court was still bound by the decision in *Smith*, the Court concluded that there was no violation of the Fourth Amendment:

> The right to be free from searches and seizures is fundamental, but not absolute … Every day, people voluntarily surrender personal and seemingly-private information to transnational corporations, which exploit that data for profit. Few

129 Ibid 9 (Leon J).
130 Ibid 10. A notice of appeal was filed on 3 January 2014 and the case is continuing.
131 959 F Supp 2d 724 (SD NY, 2013) ('*ACLU v Clapper*').
132 Ibid 735 (Pauley III J).
133 Ibid 736 (Pauley III J).
134 Ibid 38 [4] (Pauley III J).
135 Ibid 750 [33] (Pauley III J), citing Edward W Felten, 'Supplementary Declaration of Professor Edward W Felten', Submission in *American Civil Liberties Union v Office of the Director of National Intelligence*, 13-cv-03994 (WHP), 26 August 2013.
136 *ACLU v Clapper*, 959 F Supp 2d 724, 752 [33] (Pauley III J) (SD NY, 2013).

> think twice about it, even though it is far more intrusive than bulk telephony metadata collection.[137]

The section 215 and PRISM scenarios generate fundamental questions regarding the nature of privacy in the US. Does privacy exist solely in the context of the Fourth Amendment and, given the limitations in the Fourth Amendment flagged above, do these concerns need more specific protection in the digital age? This would need to take account of consumer practices and internet business models, such as the extent of personal information collected by service providers like Pandora. This would most likely require specific and targeted legislation.[138]

D UK Responses to Surveillance

UK privacy law has been complicated by the impact of the *European Convention on Human Rights* ('*ECHR*').[139] Common law evolution of privacy law under tortious and equitable principles has had to adapt to address requirements under the *ECHR*, through the *Human Rights Act 1998* (UK) c 42.[140] Privacy concepts have been dealt with under breach of confidence (equity) and the nascent doctrine of misuse of private information (tort). In addition, the UK has enacted the *Data Protection Act 1998* (UK) c 29 which implements the European Union ('EU') Data Protection Directive.[141]

The UK has been directly caught up in the outcomes of the Snowden revelations, with the UK being one of the 'Five Eyes' partners with the US, as well as revelations regarding the UK's own mass data surveillance program through the Government Communications Head Quarters.[142] However, no law reform has been proposed in the wake of the revelations, but rather a review of internet surveillance practices and their control and oversight in the UK has been

---

137 Ibid 756–7.

138 It is beyond the scope of this article to specify the shape and nature of such legislation, but for a UK based example, see Wacks, above n 87, 263–70.

139 *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953), as amended by *Protocol No 14 to the Convention for the Protection of Human Rights and Fundamental Freedoms, Amending the Control System of the Convention*, opened for signature 13 May 2004, CETS No 194 (entered into force 1 June 2010).

140 For a discussion of these developments, see also Helen Fenwick and Gavin Phillipson, *Media Freedom Under the Human Rights Act* (Oxford University Press, 2006); Gavin Phillipson, 'Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act' (2003) 66 *Modern Law Review* 726.

141 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* [1995] OJ L 281/31. For further information on proposed reforms to EU Data Protection law, see David Lindsay, 'The "Right to be Forgotten" in European Data Protection Law' in Normann Witzleb et al (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014) 290.

142 Greenwald, above n 59, 161–8.

commissioned, to be conducted by the independent think tank, Royal United Services Institute ('RUSI').[143]

A recent UK High Court decision in which Tugendhat J confirmed the existence in the UK of a tort of misuse of private information provides some useful guidance regarding how anonymous and collated data may be viewed in a privacy context in the UK: *Vidal-Hall v Google Inc*.[144] In this case three UK-based users of Google alleged that Google had misused their private information and acted in breach of confidence and their statutory duties under section 4(4) of the *Data Protection Act 1998* c 29 by tracking and collating information relating to their internet usage using the Safari browser in 2011 and 2012, such as which websites they visited, how frequently they visited the sites, how long they spent on the site and in what order sites were visited. The essence of their claim is that Google collected information from their computers, and other internet enabled devices, regarding their browsing habits. Each claimant specified in a confidential schedule their 'individual personal characteristics, interests, wishes and ambitions,' which they used as the basis of the claim that:

> they suffered distress, when they learnt that such matters were forming the basis for advertisements targeted at them, or when they learnt that, as a result of such targeted advertisements, such matters had in fact, or might well have, come to the knowledge of third parties who they had permitted to use their devices, or to view their screens.[145]

The claimants' damage is based upon the harm caused to them by the fact that their apparent interests (deduced from their browsing habits) were used to target advertising to them which disclosed certain information about them based on those interests as evidenced in their online habits. Those advertisements, and the personal information that they disclosed, may have or had been viewed by third parties viewing the claimants' devices.[146] Justice Tugendhat noted that, whilst targeted advertisements which merely reveal the employment of the user may not cause any damage:

> if the targeted advertisements apparently reveal other information about the users, whether about their personalities, or their immediate plans or ambitions, then if these matters are sensitive, or related to protected characteristics (e.g., beliefs), or to secret wishes or ambitions, then the fear that others who see the screen may find out those matters, and act upon what they have seen, may well be worrying and distressing.[147]

143 *RUSI to Convene Independent Review on the Use of Internet Data for Surveillance Purposes* (4 March 2014) RUSI <https://www.rusi.org/news/ref:N5315B2C9B1941/#.U8mvWvmSySp>.

144 [2014] EMLR 14 (Tugendhat J).

145 Ibid 349 [22] (Tugendhat J).

146 Ibid 350 [23] (Tugendhat J).

147 Ibid 350 [24].

Whilst all of the claimants claimed acute distress and anxiety, none of them claimed to have suffered any discrimination or other direct harm.[148]

Justice Tugendhat had to decide the preliminary matter of whether the claimants could serve their claim out of jurisdiction. Therefore the Court's decisions on more specific matters relating to the misuse of private information claim were of a preliminary nature only. Google was resisting the application for service outside of jurisdiction. In order to satisfy the requirements of the service out rules, the claimants framed their argument on a number of grounds including tort. With respect to this claim, Google argued that the cause of action based on misuse of private information or breach of confidence was not a tort; that no significant physical or economic harm was suffered by the claimants and the act complained of was not committed in the jurisdiction.

Whilst Tugendhat J asserted that it was clear that 'a claim for breach of confidence is not a claim in tort,'[149] the position may be different with respect to misuse of private information.[150]

Justice Tugendhat then quoted directly from Lord Nicholls in *Campbell v MGN Ltd* [2004] 2 AC 457:

> This cause of action has now firmly shaken off the limiting constraint of the need for an initial confidential relationship. In doing so it has changed its nature. In this country this development was recognised clearly in the judgment of Lord Goff of Chieveley in *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 281. Now the law imposes a 'duty of confidence' whenever a person receives information he knows or ought to know is fairly and reasonably to be regarded as confidential. Even this formulation is awkward. The continuing use of the phrase 'duty of confidence' and the description of the information as 'confidential' is not altogether comfortable. Information about an individual's private life would not, in ordinary usage, be called 'confidential'. The more natural description today is that such information is private. *The essence of the tort is better encapsulated now as misuse of private information*.[151]

Justice Tugendhat then highlighted Lord Nicholls' observation that the privacy tort and the equitable action of breach of confidence, although related,

148 Ibid 350 [25] (Tugendhat J). It should be noted that the conduct engaged in by Google during the relevant time had since been discontinued, due to regulatory sanctions brought by the United States Federal Trade Commission, which were settled in August 2012, and the outcomes of US state-based consumer actions brought by US State Attorney-Generals on behalf of 37 US states and the District of Columbia: ibid 355–6 [44]–[45] (Tugendhat J).

149 Ibid 357 [52], citing *Kitetechnology BV v Unicor GmbH Plastmaschinen* [1995] FSR 765, 777–8 (Evans LJ) ('*Kitetechnology*').

150 *Vidal-Hall v Google Inc* [2014] EMLR 14, 357 [53] (Tugendhat J). Justice Tugendhat quotes *Vestergaard Frandsen A/S v Bestnet Europe Ltd* [2010] FSR 2, 41–2 [19] where Arnold J stated that whilst breach of confidence is not a tort (citing *Kitetechnology*), '[m]isuse of private information may stand in a different position': *Campbell v MGN Ltd* [2004] 2 AC 457, 465 [14] (Lord Nicholls), in support of this suggestion: *Vidal-Hall v Google Inc* [2014] EMLR 14, 358–9 [58]–[59] (Tugendhat J).

151 *Vidal-Hall v Google Inc* [2014] EMLR 14, 358–9 [59], quoting *Campbell v MGN Ltd* [2004] 2 AC 457, 465 [14] (Lord Nicholls) (emphasis added).

should be treated separately.[152] Noting that 'there have since been a number of cases in which misuse of private information has been referred to as a tort consistently with *OBG* and these cannot be dismissed as all errors in the use of the words "tort"'.[153] Justice Tugendhat concluded 'that the tort of misuse of private information is a tort' within the meaning of the relevant rules.'[154] Therefore the claimants' claim for damages fell within the requirements of the rules relating to service out.[155]

On the question of whether the information was private, it was submitted on behalf of Google that the information collected about the claimants browsing habits was anonymous and not private:

> The aggregation of such information sent to separate websites and advertising services cannot make it private information. One hundred times zero is zero, so one hundred pieces of non-private information cannot become private information when collected together.[156]

Justice Tugendhat rejected this approach, noting that Google would not have gone to the effort to collect and collate this information unless it resulted in 'something of value'.[157] Further, he concluded the fact that individual Google employees do not identify or recognise the identity of people from whom the data is collected is 'irrelevant'.[158] At some point the claimant becomes identifiable as a

---

152 Ibid 361 [67]. Justice Tugendhat refers to *OBG Ltd v Allan* [2008] 1 AC 1, where Lord Nicholls said at 72 [255]:

> As the law has developed breach of confidence, or misuse of confidential information, now covers two distinct causes of action, protecting two different interests: privacy, and secret ('confidential') information. It is important to keep these two distinct. In some instances information may qualify for protection both on grounds of privacy and confidentiality. In other instances information may be in the public domain, and not qualify for protection as confidential, and yet qualify for protection on the grounds of privacy. Privacy can be invaded by further publication of information or photographs already disclosed to the public. Conversely, and obviously, a trade secret may be protected as confidential information even though no question of personal privacy is involved.

153 *Vidal-Hall v Google Inc* [2014] EMLR 14, 361 [68] (Tugendhat J).

154 Ibid 361 [70]. Further consideration was then given to the question as to whether the claimants had suffered any recognisable and relevant damage. Justice Tugendhat concluded that '[d]amages for distress are recoverable in a claim for misuse of private information, e.g. *Mosley v News Group Newspapers Ltd* [2008] EMLR 20': at 362 [74] (Tugendhat J).

155 Ibid 374–5 [143] (Tugendhat J). It is noted that the claimants also included a claim based upon a breach of statutory duties under the *Data Protection Act 1998*, on the basis that Google (as a 'data controller') processed their 'personal data' in breach of obligations under the data protection principles set out in the *Data Protection Act*. In particular they claimed Google had obtained 'private information' of the claimants without their knowledge or consent: *Vidal-Hall v Google Inc* [2014] EMLR 14, 353–4 [37] (Tugendhat J). The issue for the Court in this preliminary hearing was to determine if Google had in fact processed the personal data of the claimants and the judge was prepared to conclude that the matter was sufficiently arguable: As the case was concerned with the issue of service out, the data protection claim was not considered in detail.

156 Ibid 370 [115] (Tugendhat J).

157 'It would not collect and collate the information unless doing so enabled it to produce something of value. The value it produces is the facility for targeted advertising of which the Claimants complain, and which yields the spectacular revenues for which Google Inc is famous': ibid 370 [116] (Tugendhat J).

158 Ibid 117.

result of the collation and use of the information, in this case, at the point where the targeted advertisements become visible on their screen by a third party.[159] Justice Tugendhat conceded that not all of the generated information would give rise to claims of privacy. However, in the individual cases the particular types of information identified by the claimants was private information.[160]

This case illustrates the complex relationship between the concerns of privacy law and protection of private information. As is noted by the Court the argument made by Google that generic, harvested information, which can be used to generate highly detailed predictive profiles of an individual and then used to direct personally targeted information back to them, is not 'private' seems disingenuous in the specific context. Yet it is just these practices which are being used by online service providers to generate and sell targeted advertising profiles. They are based on voluntarily disclosed data, creating a contractual, but little understood, relationship with a user. As this case illustrates, further exploration of the relationships between consent, disclosure and collection and use of information is required. Further, as the law currently stands, the algorithmic intervention in such data may create a sufficient disconnect with the user to avoid any liability under privacy law. Thus law reform is needed to address these issues.

Notably, there seems to be movement in the EU on the attitudes towards mass data collection. In April 2014, the Court of Justice of the European Union held, in the joined cases C-293/12 and C-594/12,[161] that the EU Data Retention Directive[162] is invalid, on the basis that in casting the terms of the Directive, the EU legislature had exceeded the limits of the principle of proportionality in relation to Articles 7, 8 and 52(1) of the *Charter of Fundamental Rights of the European Union*.[163] The Data Retention Directive was intended to harmonise the laws of Member States with respect to the collection and retention of data generated or processed in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network, ie, internet and telephone records.[164] Data gathering on this scale was justified as essential for the purposes of national security, anti-terrorism and for the prevention of crime.[165] As with the US system

159 Ibid 371 [117] (Tugendhat J).

160 Ibid 371 [118] (Tugendhat J). He further noted: '[t]hese are not generic complaints. They are complaints about particular information about particular individuals, displayed on particular occasions (even though the precise dates and times of the occasions are not identified)': ibid 371 [119] (Tugendhat J).

161 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; Kärntner Landesregierung v Seitlinger* (European Court of Justice, C-293/12; C-59/14, 8 April 2014) [69]–[73].

162 *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC* [2006] OJ L 105/54 ('*EU Data Retention Directive*')

163 [2009] OJ C 326/391.

164 *EU Data Retention Directive* [2006] OJ L 105/54 art 1.

165 Ibid Preamble; art 1.

of data retention, the Directive authorised the collection of data related to location, time, duration of call but not content of the message or communication.[166] However, again, as has already been observed with respect to the metadata collection in the US, the European Court of Justice observed that the nature of the data collected could generate a very detailed record relating to the individuals concerned, such as their location, who they are communicating with, how and for how long and how frequently they are communicating, and the time and place of the communication.[167] Whilst the collection of such data may be justified on the basis of the general interest in the prevention of crime and national security, the Directive infringed too far upon fundamental rights to respect for private life and to the protection of personal data. The retention and use of such data would subject people to the feeling that they were under constant surveillance.[168] The effect of this decision will be to require amendment of national legislation, including that of the UK, to take account of this ruling. Notably the decision encompasses both private life (privacy) and personal data (data protection).

Shortly following this decision, the EU Data Protection Working Party adopted Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes.[169] Concluding that 'secret, massive and indiscriminate surveillance programs are incompatible with our fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security',[170] the Opinion makes a number of recommendations. These included greater transparency on how data is collected and used, clearer laws surrounding data sharing, effective oversight of intelligence services and enforcing compliance with protections and freedoms under the *ECHR*.[171] It is therefore likely that UK laws will be strengthened to reflect greater control over the use of data generated as a consequence of personal communications and transactions. Again, privacy seems a woefully inadequate tool to regulate the use of big data.

166 Ibid art 5.

167 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; Kärntner Landesregierung v Seitlinger* (European Court of Justice, C-293/12; C-59/14, 8 April 2014) [27]:

> Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.

168 Ibid.

169 'Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes' (Working Party Document No 215, Article 29 Data Protection Working Party, 10 April 2014). The Working Party was established under Article 29 of Directive 95/46/EC as an independent European advisory body on data protection and privacy.

170 Ibid 2.

171 Ibid.

IV THE AUSTRALIAN CONTEXT

Like the UK, Australian law adopts a piecemeal approach to protection of various privacy interests.[172] The *Privacy Act 1988* (Cth) is primarily concerned with data protection,[173] and imposes obligations on 'APP entities'[174] – particularly Australian government agencies, private organisations with a turnover of more than $3 million and certain small businesses[175] – regarding the collection, handling and use of 'personal information'. 'Personal information' is defined in section 6(1) of the Act as:

> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.

This limitation to an identified or reasonably identifiable individual immediately restricts its relevance in the seemingly anonymised big data context. Australian government agencies, when collecting or managing citizens' data, are also subject to a range of legislative controls, and must comply with the a number of Acts and regulations.[176] There are also many forms of overlapping and sometimes inconsistent anti-surveillance laws.[177] Protection of privacy interests may also arise in the context of the breach of confidence action, far more limited in the Australian context by the requirement of a pre-existing relationship or understanding, than in the evolving UK doctrine.[178] Additionally, there is nascent recognition of a common law tort of privacy in Australian common law.[179]

---

172 For a detailed overview of the current Australian privacy law, see Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Discussion Paper No 80 (2014) 37–50 ('*ALRC Discussion Paper*'). See also Megan Richardson and Andrew Kenyon, 'Privacy Online: Reform Beyond Law Reform' in Normann Witzleb et al (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014) 338, 340, 344–51.

173 *ALRC Discussion Paper*, above n 172, 38, para 3.3.

174 *Privacy Act 1988* (Cth) s 6(1) (definition of 'APP entity').

175 *ALRC Discussion Paper*, above n 172, 38; *Privacy Act 1988* (Cth), s 6(1) (definitions of 'agency' and 'organisation'). See also State and Territory equivalents: *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2009* (Qld); Department of the Premier and Cabinet (SA), *Information Privacy Principles (IPPS) Instruction* (2013); *Personal Information Protection Act 2004* (Tas); *Information Privacy Act 2000* (Vic).

176 See, eg, *Freedom of Information Act 1982* (Cth); *Archives Act 1983* (Cth); *Telecommunications Act 1997* (Cth); *Electronic Transactions Act 1999* (Cth); *Intelligence Services Act 2001* (Cth).

177 See *ALRC Discussion Paper*, above n 172, 41–2 [3.20]–[3.23]. See, eg, *Listening Devices Act 1992* (ACT); *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act* (NT); *Invasion of Privacy Act 1971* (Qld); *Listening and Surveillance Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA).

178 Megan Richardson, 'Towards Legal Pragmatism: Breach of Confidence and the Right to Privacy' in Elise Bant and Matthew Harding (eds), *Exploring Private Law* (Cambridge University Press, 2010) 109, 111–15, 119–23. See also *ALRC Discussion Paper*, above n 172, 68–9.

179 See *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 258 [132] (Gummow and Hayne JJ).

Recently, the Australian government has strengthened the *Privacy Act* (through the passing of the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) to enhance the protection of and set clearer boundaries for usage of personal information.[180] The Australian Law Reform Commission ('ALRC') has also recommended the introduction of a statutory cause of action for a 'serious invasion of privacy'.[181] The suggested introduction of a stand-alone tort is intended to address a range of privacy intrusions, including physical invasions of privacy and online abuses, but is not specifically directed at data privacy.[182]

The elements of the suggested tort are an 'intentional or reckless invasion of privacy' by:

(a) intrusion into the plaintiff's seclusion or private affairs (including by unlawful surveillance); or

(b) misuse or disclosure of private information about the plaintiff.[183]

The proposed action is also subject to the conditions that:

> A person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances … The court must consider that the invasion of privacy was 'serious', in all the circumstances, having regard to, among other things, whether the invasion was likely to be highly offensive, distressing or harmful to a person of ordinary sensibilities in the position of the plaintiff … The court must be satisfied that the plaintiff's interest in privacy outweighs the defendant's interest in freedom of expression and any broader public interest in the defendant's conduct.[184]

A particular issue will be the role of consent as a defence to any breach of privacy under the proposed statutory cause of action. As the ALRC Discussion Paper notes there are many degrees to consent. In particular: 'some have questioned whether clicking "I agree" to a 40 000-word term of a contract is, in fact, consent and there are calls for the whole issue of consent in the context of online services to be reviewed.'[185] The Discussion Paper suggests that this debate should occur 'in … the context of consumer protection.'[186]

---

180 *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) sch 1. See, eg, *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) sch 1 pt 1.1 (Australian Privacy Principle 1 – open and transparent management of personal information); *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) sch 1 pt 2.3 (Australian Privacy Principle 3 – collection of solicited personal information); *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) sch 1 pt 2.5 (Australian Privacy Principle 5 – notification of the collection of personal information); *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) sch 1 pt 4.11 (Australian Privacy Principle 11 – security of personal information).

181 *ALRC Discussion Paper*, above n 172, 53.

182 Ibid 54 [4.8], 76.

183 Ibid 62.

184 Ibid 62–3.

185 Ibid 97 [6.52], citing Solove, above n 11.

186 *ALRC Discussion Paper*, above n 172, 97 [6.52]. See also Richardson and Kenyon, above n 172, 349.

The proposed protection of privacy as a tort is consistent with the UK approach outlined above.[187] In addition, the ALRC contemplates that actions for breach of confidence would still continue to evolve.[188] Therefore the scope of rights against invasions of personal privacy would appear to be expanded by the ALRC proposals. However, notably, the proposed statutory right of action applies only to unlawful surveillance.[189] As Australia has no bill of rights or any constitutional protections akin to those outlined above with respect to the US, UK or EU it is unlikely that these changes will go any way to addressing the concerns regarding either government surveillance or the seemingly consensual collection of data about our online movements by platform providers with whom we 'consent' to exchange information in order to make use of their platform.

Australia is one of the Five Eyes partners with the US (along with Canada, New Zealand, and the UK) and as such is involved in the collection and sharing of intelligence information about its own citizens and those of the other Five Eyes partners. Indeed in 2011, Australia, through the Defence Signals Directorate, sought enhanced surveillance of Australian citizens due to the 'increasing number of Australians involved in international extremist activities'.[190] Commonwealth 'enforcement agencies' can request historical communications data from service providers without a warrant under the *Telecommunications (Interception and Access) Act 1979* (Cth), where the information is considered reasonably necessary for certain specified purposes including enforcement of the criminal law.[191] The total number of requests must be reported annually. For example, in 2011–12, Australian law enforcement agencies, other than the Australian Security Intelligence Organisation ('ASIO'), made 293 501 requests for telecommunications data without a warrant or any judicial oversight.[192] Unlike the CIA and the British intelligence agencies, ASIO has blanket immunity from freedom of information legislation.[193]

In 2012, following a review of national security legislation, the then Labor Australian Government announced the proposed introduction of a requirement that carriage service providers retain data regarding use of internet and phone services for up to two years.[194] In June 2013, the Parliamentary Joint Committee

187 *Vidal-Hall v Google Inc* [2014] EMLR 14, 356–63 [50]–[75] (Tugendhat J). Although the development of the tort of privacy in the UK is found in common law, the development occurred within the context of legislative change required by the *Human Rights Act 1998* (UK) c 42. In Australia specific legislative intervention would be required.

188 *ALRC Discussion Paper*, above n 172, 60 [4.33].

189 Ibid 97 [6.52], citing Solove, above n 11.

190 Greenwald, above n 59, 122. The Australian Signals Directorate (formerly the Defence Signals Directorate) is an Australian Government intelligence agency within the Department of Defence.

191 See, eg, *Telecommunications (Interception and Access) Act 1979* (Cth) ss 178, 178A, 179.

192 Attorney-General's Department, *Telecommunications (Interception and Access) Act Report for the Year Ending 30 June 2012* (2011–12) 66.

193 *Freedom of Information Act 1982* (Cth) sch 2 pt 1 div 1.

194 See also Bruce Baer Arnold, 'If Nicola Roxon Doesn't Believe in Her Own Policy, Why Should We?' *The Conversation* (online), 25 July 2012 <http://theconversation.com/if-nicola-roxon-doesnt-believe-in-her-own-policy-why-should-we-8387>.

on Intelligence and Security tabled its *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*.[195] The data retention proposals were shelved pending the federal election. In December 2013 the Senate referred a comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (Cth) to the Senate Legal and Constitutional Affairs References Committee.[196] However, the current Australian Attorney-General announced in early August 2014 that internet service providers and telecommunications providers will be required to keep user metadata for two years in order to provide access to such data by law enforcement agencies.[197] No formal procedures have yet been announced, with the proposal having only been flagged in press conferences. Some significant gaps have already been highlighted in the government's overall understanding of how such a program may work but the details remain to be worked out.[198] These proposals have attracted significant attention in light of the Snowden revelations. Again, it should be noted that as such collection involves metadata rather than the content of communications it will fall outside the scope of existing Australian privacy regimes. However, as the above analysis reveals the predictive value of such data cannot be overstated.

Recent Australian cases highlight the vulnerability of personal data collection being posted online,[199] how easily metadata can be obtained by outside

---

195 Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (2013).

196 Senate Legal and Constitutional Affairs Committee, Parliament of Australia, *Comprehensive Revision of Telecommunications (Interception and Access) Act 1979* (2013):

> On 12 December, the Senate referred the following matter to the Legal and Constitutional Affairs References Committee for inquiry and report: *Comprehensive revision of the Telecommunications (Interception and Access) Act 1979* (the Act), with regard to:
>
> - the recommendations of the Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* report, dated May 2008, particularly recommendation 71.2; and
> - recommendations relating to the Act from the Parliamentary Joint Committee on Intelligence and Security *Inquiry into the potential reforms of Australia's National Security Legislation* report, dated May 2013.

197 Emma Griffiths, 'Government Backtracks on Racial Discrimination Act 18C Changes; Pushes ahead with Tough Security Laws', *ABC News* (online), 5 August 2014 <http://www.abc.net.au/news/2014-08-05/government-backtracks-on-racial-discrimination-act-changes/5650030>; Emma Griffiths, 'Data Retention Laws: Tony Abbott Says Government "Seeking Metadata", Not Targeting People's Browsing History', *ABC News* (online), 6 August 2014 <http://www.abc.net.au/news/2014-08-06/security-laws-abbott-browsing-history-not-collected/5652364>.

198 Ben Grubb and James Massola 'What is "Metadata" and Should You Worry if Yours Is Stored by Law?' *The Sydney Morning Herald* (online), 6 August 2014 <http://www.smh.com.au/digital-life/digital-life-news/what-is-metadata-and-should-you-worry-if-yours-is-stored-by-law-20140806-100zae.html>.

199 See, eg, *Mastrangioli v Chisholm Institute of Technical and Further Education* [2014] FCA 66. All of the witnesses gave evidence of not having known that Ms Mastrangioli had been a patient at Casey and that they did not know of, and had not seen, her medical records which had been put on the internet: at [2] (Pagone J).

organisations and countries, and the lack of protection for individuals when their data collection is corrupted.[200]

Australian privacy law therefore remains, like the US and UK law, woefully underdeveloped when it comes to protection of individuals' metadata or 'voluntarily' disclosed data. Many ubiquitous, day to day disclosures of data, such as postings on Facebook, use of search terms or hash tags, likes, retweets and public polls would be regarded as public rather than private disclosures. These disclosures are then used to develop detailed algorithmic profiles, to which no privacy regulation would apply, despite potential enduring and significant impacts of that profile.

V CONCLUSIONS

Current technologies make surveillance and data capture a convenient by-product of ordinary daily transactions and interactions. Data capture is so ubiquitous that it is easier to capture it all and interrogate it later. Little regard has been had to the individual privacy interests of citizens within this context and current privacy paradigms are ill-equipped to address algorithmic and predictive uses of big data.

It must be recognised that threats to privacy can come equally from government and the private sector. The proposed US solution of ending bulk data storage by the government and transferring the responsibility to private providers carries with it the potential for continued exploitation. As demonstrated by *Vidall-Hall v Google Inc,* data mining can enable corporations to single out customers who are statistically profitable and calculate the exact minimum level to make customers loyal, therefore reinforcing the contractual power imbalances between consumers and producers.[201]

Surveillance should require 'legal process and the involvement of the judiciary to ensure that surveillance is targeted, justified, and no more extensive than is necessary'.[202] Richards asserts that

> while covert domestic surveillance can be justified in discrete (and temporary) instances when there is rigorous judicial process, blanket surveillance of all internet activity menaces our intellectual privacy and gives the government too much power to blackmail or discriminate against the subjects of surveillance.[203]

Further, the belief in the existence of constant monitoring operates as a chilling effect upon freedom of communication, deterring participation in the

200 See, eg, *Denlay v Federal Commissioner of Taxation* (2010) 81 ATR 644; *Denlay v Federal Commissioner of Taxation [No 2]* (2011) 83 ATR 872 (dealing with illegally obtained information affecting a tax assessment).

201 See, Palmås, above n 3, 349.

202 Richards, above n 1, 1961.

203 Ibid.

democratic process.[204] In a free society, all forms of surveillance must be ultimately accountable to a self-governing public. Statutory law is easily adaptable and can be applied to bind both government and non-government actors. Accordingly, a meaningful legal process of issuing a warrant supported by probable cause needs to be followed before the government can perform the digital equivalent of reading our diaries or worse, making a decision on the basis of casting our horoscopes.

It is important to follow the rule of law and have a member of the judiciary provide independent oversight of the use of coercive or invasive powers of data collection. Otherwise, the collection of big data is unhindered and unreviewable which undermines democracy. In addition, a statutory right to prevent misuse of information linked to or generated about a person from big data by both government and business would go some way to protect individual privacy. However, this would also necessitate significant changes to current internet-based business models to prevent the bulk exploitation of *our* bulk data. Change is needed now to address these issues, before the rampant algorithms make it impossible to claw back what little privacy we retain in the online environment.

204 Ibid 1945.