TAMING THE ELECTRONIC GENIE: CAN LAW REGULATE THE USE OF PUBLIC AND PRIVATE SURVEILLANCE?

STEPHEN GRAY* AND YEE-FUI NG**

The fear that our social and legal institutions are being subtly but inexorably eroded by the growth in surveillance is as common in academic literature as it is in the popular imagination. While large corporations harness the powers of Big Data for the wholesale harvesting of personal data, the government utilises its coercive powers to conduct increasingly intrusive surveillance of members of the public. The article considers the major issues arising from private surveillance, particularly the breaches of privacy inherent in the collection or harvesting of personal information. It then analyses selected issues arising from public surveillance, including data retention and sharing by government, the use of surveillance techniques such as facial recognition technology in criminal investigation, and the evocation of national security concerns to justify invasions of privacy. It considers what legal regime is best suited to regulate mass public and private surveillance, including the tort of privacy, the adoption of international regimes, such as the General Data Protection Regulation, and the expansion of fiduciary principles. We argue that the concept of 'information fiduciary' should be added to the current range of measures designed to ensure the accountability of both public and private data collectors.

* Senior Lecturer, Faculty of Law, Monash University.

** Associate Professor, Faculty of Law, and Acting Director, Australian Centre for Justice Innovation, Monash University.

The authors would like to thank Moira Paterson and Normann Witzleb for their helpful comments on a draft of this article. We also wish to thank the anonymous referees and reviewers of this article.

I INTRODUCTION

Is it possible for law to restrain the excesses of the 'surveillance state',[1] and its accompanying private version 'surveillance capitalism', the result of a 'Fourth Industrial Revolution'[2] in digital technology which, according to its critics, poses a fundamental threat to the rule of law?[3] The question is difficult to answer, because it is difficult, if not impossible, to quantify the nature of the threat. Surveillance may not itself be secret, but its results in the form of data or information are likely to be used in unknown or unquantifiable ways. The ordinary citizen has no way of knowing to what extent they are being tracked in public or private spaces, their online behaviour is monitored by public or private agencies, their data is retained and shared with unknown entities, or used for profit, or their behaviour or values being subtly modified, perhaps even fundamentally altered.[4] Perhaps the fear that we are being watched is exaggerated, or perhaps, as Zuboff maintains, that thought is itself a measure of how far our senses have been numbed, our behaviour conditioned, our perception of the threat dulled by the overwhelming nature of the threat itself.[5]

This fear, that our social and legal institutions are being subtly but inexorably eroded by the growth in surveillance, is as common in academic literature as it is in the popular imagination. As this literature repeatedly notes, there is an urgent concern that we are experiencing an 'erosion of core aspects of individual privacy',[6] or even have arrived at 'the end of privacy'.[7] It has even been suggested that this may 'fundamentally alter the nature of human behaviour and interaction, our sense of personal freedom and the ethos of democratic societies'.[8] Amongst the many dangers inherent in this erosion of privacy is the harm to autonomy

1 For an example from early 2021 of the use of this term, see Paul Gregoire, 'Why Are Australian Governments Constructing the Surveillance State?', *Sydney Criminal Lawyers* (Blog Post, 1 January 2021) <https://www.sydneycriminallawyers.com.au/blog/why-are-australian-governments-constructing-the-surveillance-state/>.

2 Matt Bartlett, 'Beyond Privacy: Protecting Data Interests in the Age of Artificial Intelligence' (2021) 3(1) *Law, Technology and Humans* 96, 96 ('Beyond Privacy').

3 For example, Friedland argues that invisible mass surveillance 'has threatened privacy, particularly privacy's role as a structural check on indiscriminate and illegitimate government action': Steven I Friedland, 'Privacy and Democracy in the Digital Age' (2015) 20(1) *Media and Arts Law Review* 1, 14.

4 See, eg, discussion in Bartlett, 'Beyond Privacy' (n 2) 97–9.

5 According to Zuboff, ordinary life is now so deeply immersed and saturated in the machinery of surveillance capitalism, and our dependency on it so total, that it 'produces a psychic numbing that inures us to the realities of being tracked, parsed, mined, and modified': Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019) 11.

6 Konrad Lachmayer and Normann Witzleb, 'The Challenge to Privacy from Ever Increasing State Surveillance: A Comparative Perspective' (2014) 37(2) *University of New South Wales Law Journal* 748, 749.

7 Simon Chesterman, *One Nation under Surveillance: A New Social Contract to Defend Freedom without Sacrificing Liberty* (Oxford University Press, 2011) 1.

8 Lachmayer and Witzleb (n 6) 749.

through loss of control of one's personal information and the consequent potential for manipulation; harm to human dignity including the potential for discrimination; and the loss of personal anonymity.[9]

Almost as pervasive in the literature is the sense that the law has failed to keep up with the challenges posed by public and private surveillance. In part, the reasons for these legal shortcomings are philosophical. The common law has a traditional hostility towards a legal conception of privacy, exemplified in Bagaric's comment that: 'A strong right to privacy is no more than a request for secrecy — refuge of the guilty, paranoid and misguided, none of whom should be heeded in sorting through the moral priorities of the community.'[10] In part, the reasons for the law's failure are historical, the product of the fact that the principles of information privacy 'developed in an age where technology and data simply did not exist in the way they do now',[11] with its main tenets in Australia, New Zealand and the European Union ('EU') developing from a framework recommended by the Organisation for Economic Cooperation and Development ('OECD') in 1980.[12]

In part, it is the product of the nature of the electronic world, whose major players 'such as Google move faster than the state's ability to understand or follow'.[13] Arguably, and more controversially, these powerful players are characterised by a 'contempt for law and regulation',[14] and a willingness to lobby against the efforts of government or citizens to limit their power.[15] At least on occasions, the efforts of these corporate entities are aided and abetted by elements of government, in particular the security agencies, whose interests in secrecy and large-scale information-gathering coincide with theirs.[16]

This article considers what addition to the current legal regimes, if any, may be best suited in Australia to tame the electronic genie of mass public and private surveillance, and the uses to which the information gathered thereby is put. Due to the complexity, variety and volume of the laws scrutinised, our focus will be on

9 For discussion of the harms arising from the loss of privacy, see Moira Paterson and Maeve McDonagh, 'Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data' (2018) 44(1) *Monash University Law Review* 1, 6–9.

10 Mirko Bagaric, 'Privacy Is the Last Thing We Need', *The Age* (online, 22 April 2007) <https://www.theage.com.au/national/privacy-is-the-last-thing-we-need-20070422-ge4pur.html>.

11 Bartlett, 'Beyond Privacy' (n 2) 100.

12 Organisation for Economic Co-operation and Development, *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD/LEGAL/0188, 23 September 1980); ibid 99.

13 Zuboff (n 5) 104.

14 Ibid 105.

15 Ibid 125.

16 According to Zuboff, there is an 'elective affinity between public intelligence agencies and the fledgling surveillance capitalist Google', which 'sustained surveillance exceptionalism and contributed to the fertile habitat in which the surveillance capitalism mutation would be nurtured to prosperity': ibid 115.

the federal level, although we note that the states have their own privacy and surveillance legislative schemes. Part II will define surveillance and briefly set out the historical and legal conditions which led to the exponential growth in its use. Part III will consider the major issues arising from private surveillance, particularly the breaches of privacy inherent in the expropriation of information and experience as 'free raw material for translation into behavioural data'[17] as well as some of its starkest political effects, including voter manipulation, and the commercial and consequently cultural impoverishment of traditional news media.

Part IV will consider several of the most significant and controversial recent issues arising from public surveillance. These will include the retention of data by government, the use of surveillance techniques such as facial recognition technology ('FRT') in criminal investigation, and the evocation of national security concerns to justify breaches of privacy, with consequent effects on media and individual freedom. Part V will briefly consider various legal regimes proposed to address the issues arising from surveillance, including a common law tort of privacy, an equitable action for breach of confidence, and a data retention right. Part VI will argue that the notion of an 'information fiduciary', first proposed in the United States,[18] could be adapted to the Australian context, supplementing and working alongside the existing regimes to provide a better balance between the interests of those who carry out surveillance and those who are its subjects.

II THE NATURE AND ORIGINS OF THE 'SURVEILLANCE STATE'

'Surveillance' is not a legal term of art. With its origin in the French *surveiller*, meaning to watch over,[19] it may be defined as 'the organized observation of behaviour with the intention of care or control of the observed',[20] or, more pointedly, as the 'focused, systematic and routine attention to personal details for purposes of influence, management, protection, or direction'.[21] However, it is generally left undefined, at least in Australian statutes addressing civil surveillance.[22] It 'may be overt or covert', and may take the form of listening or audio surveillance, optical or visual surveillance, data surveillance, tracking or location surveillance, and biometric surveillance, which is 'the collection [and] recording of biological samples [or] physical or behavioural characteristics'.[23] It

17 Ibid 8.

18 Jack M Balkin, 'Information Fiduciaries and the First Amendment' (2016) 49(4) *UC Davis Law Review* 1183.

19 Friedland (n 3) 2.

20 Mark B Salter, 'Surveillance' in J Peter Burgess (ed), *The Routledge Handbook of New Security Studies* (Routledge, 2010) 187, 187.

21 Ibid 187–8, quoting David Lyon, *Surveillance Studies: An Overview* (Polity, 2007) 14.

22 Peter Leonard, 'Critically Surveying Civil Surveillance Statutes in Australia' (2020) 17(6) *Privacy Law Bulletin* 111.

23 Ibid 112.

may be public or private. In its public form, that is, when carried out by government or government agencies, it includes 'internet surveillance, video surveillance of public spaces, electronic eavesdropping, data retention, monitoring of bank accounts and social media, the sharing of air travel booking information, large scale intrusions into email, web chat and data held in cloud storage'.[24] In its private form, that is, when carried out by private individuals or corporations, it includes many of the forms just listed, but also surveillance of everyday experiences such as using health services, buying products online, encountering paparazzi, or being at work.[25] The legal landscape is extremely crowded. Hundreds of Australian statutes feature privacy provisions, or are concerned with privacy and data protection.[26]

While the legal detail is complex, the academic literature makes one general point, which is in any case an obvious feature of everyday 21st century experience: that the use of public and private surveillance has grown exponentially, touching every aspect of most Australians' daily lives. Chesterman refers to the 'revolution in technology and communications', and the 'increased use of electronic communications … matched by the development of ever more sophisticated tools of surveillance', accompanied with 'changes in culture' that have 'progressively reduced the sphere of activity that citizens can reasonably expect to be kept from government eyes'.[27] He speaks of the 'battleground of privacy' being a war bound to be lost, because of the government's increased ability to collect information, and the citizens' increasing acceptance 'that they *will* collect it'.[28] Lachmayer and Witzleb write of the 'massive surveillance of ordinary citizens on an unprecedented scale by law enforcement and national security agencies',[29] while Bartlett, speaking of private surveillance and data collection, refers to the 'challenge to privacy … amplified by the new-found ability of AI to influence actual behaviour, far beyond the realm of advertising'.[30] Friedland refers to a world of 'multiple mass surveillance systems, expanding regularly by the advances of Big Data and evolving technology'.[31] As the Australian Competition and Consumer

24 Lachmayer and Witzleb (n 6) 749.

25 B Arnold, LexisNexis, *Privacy, Confidentiality and Data Security in Australia* (online at 14 February 2023) [1000].

26 Australian Law Reform Commission, 'Review of Australian Privacy Law' (Discussion Paper No 72, September 2007) vol 1, 145–68.

27 Chesterman (n 7) 3.

28 Ibid 4 (emphasis in original).

29 Lachmayer and Witzleb (n 6) 749.

30 Bartlett, 'Beyond Privacy' (n 2) 98.

31 Friedland (n 3) 4. Big Data involves the 'use of analytical tools based on artificial intelligence and machine learning to mine the vast data troves being gathered and accumulated at ever increasing rates': Paterson and McDonagh (n 9) 1.

Commission's ('ACCC') *Digital Platforms Inquiry* of 2019 observes, '90 per cent of all the data that exists in the world today was created in the last two years'.[32]

Lachmayer and Witzleb locate the origins of this exponential growth in the September 11, 2001 ('9/11') terrorist attacks, which led to increasing challenges to '[l]ong-held and cherished principles relating to democracy, the rule of law and the protection of a wide range of human rights'.[33] Speaking of the growth in surveillance powers wielded by security agencies, Chesterman similarly refers to an increasing disregard for traditional notions of the rule of law 'following the September 11 attacks on the United States'.[34] David Lyon writes of 'a sharp tilt towards more exclusionary and intrusive surveillance practices' following the 9/11 attacks, with '[e]xisting surveillance practices … being intensified, and previous limits … lifted'.[35]

In an influential recent account, Zuboff has argued that increasing social inequality in Western liberal democracies, coupled with increasing emphasis on 'psychological individuality' amongst ordinary citizens, has created a type of 'cultural vacuum';[36] or an 'existential contradiction of the second modernity that defines our conditions of existence: we want to exercise control over our own lives, but everywhere that control is thwarted'.[37] Into this vacuum, in Zuboff's account, stepped Google and Facebook, the major players of the internet age.[38] She terms their practices a 'voracious and utterly novel commercial project' which she dubs 'surveillance capitalism',[39] a 'rogue force driven by novel economic imperatives that disregard social norms and nullify the elemental rights associated with individual autonomy'.[40] This form of capitalism feeds, not on labour, as did Karl Marx's image of industrial capitalism, but on 'every aspect of every human's experience',[41] which is unilaterally claimed as 'free raw material for translation into behavioral data'.[42] This raw data is fed, not so much into product or service improvement, as was the early promise, but into machine intelligence used for

32 Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019) 379 ('*Digital Platforms Inquiry*'), citing James Dipple-Johnstone, 'Regulating the Tech Giants in the Digital Age' (Beesley Lecture, Institute of Directors, 31 October 2018).

33 Lachmayer and Witzleb (n 6) 748.

34 Chesterman (n 7) 9.

35 David Lyon, *Surveillance after September 11* (Polity, 2003) 7.

36 Zuboff (n 5) 37.

37 Ibid 45.

38 Ibid 33.

39 Ibid 7 (emphasis omitted).

40 Ibid 11.

41 Ibid 9.

42 Ibid 8.

prediction of future behaviour, which is traded in a marketplace she terms the 'behavioral futures markets'.[43]

Most significantly for our purposes, Zuboff argues that there is an 'absence of law to impede their progress', as well as a 'mutuality of interests between the fledgling surveillance capitalists and state intelligence agencies'.[44] This means that government has little interest in seriously impeding its activities. Before 9/11, she contends, elements in government were active in advocating for legislation that 'would have protected consumers online', including '"clear and conspicuous" notice of information practices; consumer choice over how personal information is used; access to all personal information, including rights to correct or delete; and enhanced security of personal information'.[45] After the New York attacks, the focus shifted overwhelmingly to security rather than privacy, 'thrust[ing] the intelligence community into an unfamiliar demand curve that insisted on exponential increases in velocity'.[46] Both the security agencies and Google were successful in achieving a legal landscape in which surveillance and expropriation of data could proceed unimpeded.[47]

Zuboff's account is arguably hyperbolic,[48] and the extent to which it is an offshoot of broader relationships between capital and labour is highly debatable. However, we argue that she has articulated important underlying themes in the development of the data economy, and particularly the dystopian fear — that we are being remorselessly analysed, stripped and picked over, anaesthetised to the true extent of our plight — which ultimately drives the law's efforts to identify and rein in the excesses of the surveillance state.

43 Ibid (emphasis omitted).

44 Ibid 19.

45 Ibid 113, citing Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (Report, May 2000) 36–7.

46 Zuboff (n 5) 115.

47 In the United States context, Zuboff argues that First Amendment judicial reasoning abetted this process, partly by protecting hate speech and pornography as aspects of freedom of expression, as well as shielding the online platforms from liability for racist or inflammatory content, but also by asserting a 'close connection between free speech and property rights', and thus preventing 'any form of oversight or externally imposed constraints that either limit the content on their platforms or the "algorithmic orderings of information" produced by their machine operations': ibid 109, quoting Frank Pasquale, 'The Automated Public Sphere' (Legal Studies Research Paper No 2017-31, Francis King Carey School of Law, University of Maryland, 8 November 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3067552>.

48 Fleur Johns terms it a 'jeremiad', full of '[o]missions, elisions, romantic fantasies, and psychoanalytic tropes', a simplification of a complex reality into a 'singular, spectral Lacanian figure', the '"sensate, computational, connected puppet that renders, monitors, computes, and modifies human behaviour"': Fleur Johns, '"Surveillance Capitalism" and the Angst of the Petit Sovereign' (2020) 71(5) *British Journal of Sociology* 1049, 1050–1, quoting Zuboff (n 5) 376.

The next section will look at private surveillance — particularly, the legal issues arising from the extraordinary market power of internet companies, and their use of private 'behavioral data' for commercial purposes.

III PRIVATE SURVEILLANCE

While older, visual forms of surveillance remain significant, it is clear that surveillance by means of data gathering is the dominant form of the digital age. It consists of the vast volume of information gathered unceasingly by 'Big Data' companies from the mobile phones and other devices of private citizens, including now smart devices with physical functions, such as a watch, a thermostat or a kitchen appliance', all of which provide a 'multitude of data-driven feedback and calibration'.[49] Such devices, collectively now known as the 'Internet of Things', add substantially to the pool of data available due to association of individuals with objects that can be tracked on the internet and provide an increasingly 'clearer picture of what [citizens] do in [their] private lives'.[50] This data is available not just to the private companies which collect them, but to anybody else, public or private, to whom they choose to sell or exchange the data, effectively creating a 'revolving door', with 'little regard for the purposes for which [the data] was originally collected'.[51] While it is true that consumers typically sign online consent forms permitting secondary use of data in exchange for access to the relevant platform, there is a clear 'imbalance of power … between the data subject and the data controller',[52] an imbalance characterised by Margaret Radin as a degradation of the rule of law itself.[53]

Friedland argues that there is a lack of narrative concerning the personal harm done by this systemic violation of privacy, making it 'more difficult to distinguish between legitimate and illegitimate powers, creating a slippery slope of one-sided justification'.[54] It is fundamental that protecting personal information is a precondition to the protection of privacy, and in turn to other human rights. From this it follows that

49 Friedland (n 3) 5.

50 Ibid.

51 Judith Rauhofer, 'Round and Round the Garden? Big Data, Small Government and the Balance of Power in the Information Age' (2015) 8(1) *Journal of Law and Economic Regulation* 34, 43, quoted in Paterson and McDonagh (n 9) 13–14. See also Bart Custers and Helena Uršič, 'Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection' (2016) 6(1) *International Data Privacy Law* 4.

52 Paterson and McDonagh (n 9) 14. The Australian Competition and Consumer Commission ('ACCC') characterised such contracts as 'standard-form click-wrap agreements with take-it-or-leave-it terms and bundled consents, which limit the ability of consumers to provide well-informed and freely given consent to digital platforms' collection, use and disclosure of their valuable data': *Digital Platforms Inquiry* (n 32) 23.

53 Margaret Jane Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton University Press, 2012) pt 1.

54 Friedland (n 3) 6.

> Big Personal Data is harmful to privacy because it removes the ability of individuals to exercise control over their own individual data, thereby undermining their autonomy (ie 'living and ordering a life of one's own choosing').[55]

Zuboff puts a similar point more colourfully. She likens surveillance capitalists to the Spanish Conquistadors, who legitimised their invasion by means of declarations, presenting as completed fact that which they hoped to achieve.[56] With this analogy, she characterises the ordinary consumer as akin to South American Indigenous people, who were completely unable to process or understand the momentous significance of the Spanish arrival, because it was so utterly foreign to the world they had understood hitherto.[57]

Much of the academic literature in this area focuses on the implications for privacy rights.[58] Central to the issue of privacy in this context are the uses to which the 'vast troves of personal data' are put.[59] However, privacy regulation is often concerned with the input (ie which data a person can use and for what purpose), but there are additional concerns about regulating the output (ie how we can avoid discrimination and manipulation resulting from data processes). As Paterson and McDonagh point out, the 'social richness of Big Personal Data allows inferences about matters such as people's personalities, and can assist in identifying personal weaknesses which can potentially be exploited to manipulate their behaviour'.[60] Not just personal weaknesses, but information about all forms of behaviour and personal choices, as well as inherent characteristics, may be collected and manipulated in a way that is very difficult, if not actually impossible, to regulate, because of the complexity and vast scale of the processes involved.[61]

Of course, it is important to acknowledge that some of this data harvesting is benign in nature. In a defence of 'Big Data', and of the 'Internet of Things', MacCarthy argues that machine learning and artificial intelligence will 'transform everyday life … creating enormous opportunities and challenges',[62] referring to

55 Paterson and McDonagh (n 9) 7, quoting Mark Hickford, New Zealand Law Commission, *A Conceptual Approach to Privacy* (Miscellaneous Paper No 19, October 2007) 5 [4.2]. See also the discussion of the importance of privacy in Jelena Gligorijevic, 'A Common Law Tort of Interference with Privacy for Australia: Reaffirming *ABC v Lenah Game Meats*' (2021) 44(2) *University of New South Wales Law Journal* 673, 683–6.

56 'Conquest by declaration should sound familiar because the facts of surveillance capitalism have been carried into the world on the strength of six critical *declarations* pulled from thin air when Google first asserted them.': Zuboff (n 5) 179 (emphasis in original).

57 Ibid 12, 178–9.

58 See, eg, Friedland (n 3).

59 Paterson and McDonagh (n 9) 1.

60 Ibid 8, citing Renaud Lambiotte and Michal Kosinski, 'Tracking the Digital Footprints of Personality' (2014) 102(12) *Proceedings of the IEEE* 1934.

61 See, eg, the discussion in Paterson and McDonagh (n 9) 14.

62 Mark MacCarthy, 'In Defense of Big Data Analytics', in Evan Selinger, Jules Polonetsky and Omer Tene (eds), *The Cambridge Handbook of Consumer Privacy* (Cambridge University Press, 2018) 47, 49. See also Paterson and McDonagh (n 9) 5–6.

the beneficial impact of data harvesting on the development of driverless cars, on speech recognition software, and in health care.[63] He acknowledges 'the dangers of computer surveillance and information misuse', but considers these outweighed by the gains, arguing that we must 'retain and analyze truly staggering amounts of information. It is now sensible to retain this information rather than routinely discarding it.'[64] He argues that it is neither possible nor desirable to regulate secondary uses of data requiring full notice and consent for all such uses, advocating instead for a 'risk analysis of secondary uses to assess likely harms and benefits'.[65] Such an analysis would presumably need to be undertaken by the data collector — a good example, arguably, of the fox being set to guard the henhouse.

It is no doubt true that there are social benefits to 'Big Data' harvesting of personal information, beyond the enormous wealth accrued to the harvesters themselves.[66] However, we suggest that in many contexts there is evidence that these benefits may be outweighed by the dangers. Since 2010, Facebook and other 'Big Data' harvesters have increasingly understood the power of the seemingly innocuous pieces of personal information revealed on social media in the form of likes, exclamation marks, or lists of favourite TV shows. They realised that 'Facebook profiles are not idealized self-portraits, as many had assumed',[67] but in fact reflect the user's real personality, and in a more accurate form than orthodox psychometric testing. In 2013, a study revealed that Facebook 'likes' could be used to '"accurately estimate a wide range of personal attributes" … including sexual orientation, ethnicity, religious and political views, personality traits, intelligence, [and] happiness'.[68]

The use and commercialisation of this information for targeted advertising is well known,[69] as are the particular impacts of such practices on children.[70] However,

63 MacCarthy (n 62) 49–51.

64 Ibid 56.

65 Ibid 57.

66 As the ACCC points out, 'the leading digital platforms are some of the world's most valuable listed companies', with Facebook having a market capitalisation of USD517.6 billion, and Google's parent company having a market capitalisation of USD754.2 billion, as at 17 June 2019: *Digital Platforms Inquiry* (n 32) 42.

67 Zuboff (n 5) 272.

68 Ibid 274, quoting Michal Kosinski, David Stillwell and Thore Graepel, 'Private Traits and Attributes Are Predictable from Digital Records of Human Behaviour' (2013) 110(15) *Proceedings of the National Academy of Sciences of the United States of America* 5802, 5802.

69 For a discussion of the value of the high-quality data collected by Facebook, see *Digital Platforms Inquiry* (n 32) 86–7. For a similar discussion related to Google: see at 88–9.

70 As Leaver points out, 'when an Instagram user becomes a legal adult, all of their data collected up to that point will then likely inform an incredibly detailed profile which will be available to facilitate Facebook's main business model: extremely targeted advertising': Tama Leaver, 'Instagram's Privacy Updates for Kids Are Positive: But Plans for an Under-13s App Means Profits Still Take Precedence', *The Conversation* (online, 3 August 2021) <https://theconversation.com/instagrams-privacy-updates-for-kids-are-positive-but-plans-for-an-under-13s-app-means-profits-still-take-precedence-165323>.

other more subtle and sinister forms of manipulation are perhaps less generally understood. One such form is the use of data to influence voter behaviour and election results. Facebook appears to have experimented with this practice during the 2010 United States Congressional elections, when the company positioned voting-related information next to images of selected users' Facebook friends to see whether this form of manipulation 'made a statistically significant difference in the number of users who chose to vote'.[71] The answer was that it made a significant, indeed dramatic, difference, with Facebook calculating that their intervention led to approximately 340,000 additional votes.[72]

This early intervention was relatively benign, because it merely involved encouraging people to vote, rather than attempting to influence voting behaviour. However, later exercises in voter manipulation were certainly far from benign. Of these, perhaps the best known were undertaken by British consulting firm Cambridge Analytica, which first pioneered the harvesting and manipulation of data about opposition party supporters during a general election in Trinidad. They were paid by one of Trinidad's two major parties for their campaign to encourage apathy among these supporters — a successful campaign, at least until they were caught.[73] Later applications of the company's personality-based 'micro-behavioral targeting' occurred, famously, during the 'Leave' campaign in the lead-up to the 2016 Brexit vote, and in support of Donald Trump during the 2016 US presidential election.[74]

Such overt forms of voter manipulation may be less likely in the future, following the extensive adverse publicity showered on the social media giants and their smaller private offshoots in the wake of these scandals. At the very least, Facebook has conceded that 'we also made mistakes, there's more to do, and we need to step up and do it',[75] and the company has promised various measures to 'fight the

71 Bartlett, 'Beyond Privacy' (n 2) 99.

72 Robert Bond et al, 'A 61-Million-Person Experiment in Social Influence and Political Mobilization' (2012) 489(7415) *Nature* 295, 297.

73 Paul Hilder, '"They Were Planning on Stealing the Election": Explosive New Tapes Reveal Cambridge Analytica CEO's Boasts of Voter Suppression, Manipulation and Bribery', *openDemocracy* (online, 28 January 2019) <https://www.opendemocracy.net/en/dark-money-investigations/they-were-planning-on-stealing-election-explosive-new-tapes-reveal-cambridg>. See also discussion in Bartlett, 'Beyond Privacy' (n 2) 99.

74 Zuboff (n 5) 278. See also Paterson and McDonagh (n 9) 8; Jamie Doward and Alice Gibbs, 'Did Cambridge Analytica Influence the Brexit Vote and the US Election?', *The Guardian* (online, 5 March 2017) <https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridge-analytica-what-role-brexit-trump>.

75 Mark Zuckerberg, (Facebook, 22 March 2018, 6:36am AEDT) <https://www.facebook.com/zuck/posts/10104712037900071>, quoted in Matt Bartlett, 'Facebook Reforms Not Good Enough', *Newsroom* (online, 7 July 2020) <https://www.newsroom.co.nz/ideasroom/facebook-reforms-not-good-enough>. See also Normann Witzleb, Moira Paterson and Janice Richardson (eds), *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-Targeting* (Routledge, 2020). For further general discussion of this issue, see Normann Witzleb et al (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014).

spread of false news'[76] — ironically, a phrase popularised by the figure most generally associated with that commodity, former President Donald Trump. While Google and Facebook have, indeed, taken steps to improve the reliability, trustworthiness and provenance of the information available on their platforms, there remains a significant risk of 'consumers being exposed to serious incidents of disinformation — false or inaccurate information deliberately created to harm a person, social group, organisation or country', as the ACCC has pointed out.[77]

However, Facebook's business model, or rather the inherent tendency of social media, has an equally powerful, if more subtle effect on political discourse. This is the polarising tendency of political communication on social media — that is, the tendency for people to see only communications from a political standpoint with which they already agree. This is the product of 'Facebook's desire to show users "relevant" ads' in order to keep people on the platform, an economic imperative from Facebook's point of view, but which operates 'in favor of a certain kind of political communication, the kind that focuses on engaging with people who are already on your side'.[78]

Other forms of data harvesting and manipulation raise almost equally troubling questions for the democratic process and the ideal of equality before the law. Paterson and McDonagh highlight the discriminatory implications of decision-making based on such data, for example 'fine-grained distinctions between individuals which are then used as a basis for differential treatment'.[79] Such information may be used by private companies, as by government, in a way that discriminates against minority groups, for example in the use of statistically-generated predictions about the risk of terrorism to generate no-fly lists on planes.[80]

Another serious threat to rule of law and democratic values stems from the market power exercised by 'Big Data' companies. As is well known, the rise of digital platforms, in particular Google and Facebook, has dramatically increased the fall in advertising revenue suffered by traditional news media from the beginning of

76 Adam Mosseri, 'Working to Stop Misinformation and False News', *Meta for Media* (Blog Post, 7 April 2017) <https://www.facebook.com/formedia/blog/working-to-stop-misinformation-and-false-news>. See also Normann Witzleb and Moira Paterson, 'Micro-Targeting in Political Campaigns: Political Promise and Democratic Risk' in Uta Kohl and Jacob Eisler (eds), *Data-Driven Personalisation in Markets, Politics and Law* (Cambridge University Press, 2021) 223.

77 *Digital Platforms Inquiry* (n 32) 21.

78 Gilad Edelman, 'How Facebook's Political Ad System Is Designed to Polarize', *Wired* (online, 13 December 2019) <https://www.wired.com/story/facebook-political-ad-system-designed-polarize>. See also Bartlett, 'Facebook Reforms Not Good Enough' (n 75).

79 Paterson and McDonagh (n 9) 8.

80 Ian Kerr and Jessica Earle, 'Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy' (2013) 66 *Stanford Law Review* 65, 67–8.

the internet.[81] This has had a particularly strong impact on local and regional news providers.[82] Consumers increasingly access their news media through Google and Facebook,[83] making these 'Big Data' entities 'critical and unavoidable partners' for traditional news media,[84] and placing them in a privileged bargaining position, given the substantial fall in revenue the traditional media businesses would suffer if they did not allow referrals (ie links) from Google to their websites.[85] The effect of this huge transfer in revenue from the traditional media organisations that find and write the news, to the data companies that distribute it,[86] has not only been to impoverish the 'old' organisations but it also reduces the ability of these organisations to write original and high-quality stories, particularly investigative reporting. In turn, this impoverishes the quality of information available to ordinary citizens,[87] reducing the likelihood that corruption will be exposed, or that governments and other powerful people or organisations will be held to account. Needless to say, this has significant adverse implications for 'the healthy functioning of the democratic process'.[88]

To its credit, the Australian government has attempted to address this highly significant by-product of the information-harvesting abilities of the large data companies, and their consequent enormous market power. Following the concerns expressed by traditional news media over a number of years, in December 2017, the Treasurer asked the ACCC to conduct an inquiry into 'the impact of platform service providers on media and advertising markets'.[89] In June 2019, the ACCC produced its final report,[90] with the government releasing its response to that inquiry on 12 December 2019.[91] In April 2020, the federal government 'announced that it had directed the ACCC to develop a mandatory code of conduct to address bargaining power imbalances between Australian news media businesses and

81 Classified advertising revenue earned by traditional news media declined from $2 billion in 2001 to $200 million in 2016; or with figures adjusted for inflation, from $3.7 billion to $225 million over the same period: *Digital Platforms Inquiry* (n 32) 17. 'Google and Facebook [now] receive the majority of online advertising revenue in Australia': at 119.

82 Ibid 1.

83 As the *Digital Platforms Inquiry* points out, 'Google is the largest source of referrals for websites of print/online and online only news media businesses … Facebook is the largest source of referrals for websites of radio news media businesses': ibid 101.

84 Ibid 1.

85 Ibid 101.

86 '[D]igital platforms do not directly produce journalism within Australia': ibid 51.

87 For example, 'the number of journalists in traditional print media businesses fell by 20 per cent from 2014 to 2018': ibid 18.

88 Ibid 1.

89 *Digital Platforms Inquiry* (n 32) app A.

90 *Digital Platforms Inquiry* (n 32).

91 Commonwealth, *Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (Report, 12 December 2019) ('*Regulating in the Digital Age*') <https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf>.

digital platforms',[92] with a draft code being released in July of that year.[93] There was significant and powerful opposition to the code from the 'Big Data' companies,[94] including a decision by Facebook to block Australians from access to news on its platform, a decision that was soon reversed.[95] In mid-February 2021, Google struck a number of deals with Australian media companies, reportedly worth tens of millions of dollars, with Facebook reportedly also making significant deals.[96] Legislation implementing the *News Media and Digital Platforms Mandatory Bargaining Code* ('*News Media Bargaining Code*') was passed on 25 February 2021.[97]

The Code is applicable to media companies that provide 'news' that appear on search engines or social media, providing their revenue is at least $150,000 per year.[98] The Treasurer may 'designate' digital platforms such as Google and Facebook following an assessment that there is a significant power imbalance in favour of such a platform against publishers, and with a 30-day notice period.[99] The platform must then negotiate with the media company over how much to pay

92 Australian Competition and Consumer Commission, *Mandatory News Media Bargaining Code* (Concepts Paper, 19 May 2020) 1 ('*Mandatory News Media Bargaining Code*').

93 Exposure Draft, Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020 (Cth). See also Australian Competition and Consumer Commission, *Q&As: Draft News Media and Digital Platforms Mandatory Bargaining Code* (Report, July 2020) ('*Draft News Media and Digital Platforms Mandatory Bargaining Code*').

94 The companies argued, for example, that being 'require[d] to pay for links is incompatible with "the free and open internet" and risks "breaching a fundamental principle of the Internet"': Gilbert + Tobin, 'The News Media Bargaining Code Is Now Law' (31 March 2021) *Nod and a Wink* <https://www.gtlaw.com.au/knowledge/nod-and-a-wink>, quoting Vint Cerf, Submission No 1 to Senate Standing Committees on Economics, Parliament of Australia, *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020* (10 January 2021) 3 and Sir Tim Berners-Lee, Submission No 46 to Senate Standing Committees on Economics, Parliament of Australia, *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020* (18 January 2021) 1.

95 See, eg, Jack Snape, 'The Media Bargaining Code Has Passed Parliament, but Don't Rule out Another Facebook News Ban Yet', *ABC News* (online, 24 February 2021) <https://www.abc.net.au/news/2021-02-24/news-media-bargaining-code-passes-parliament-facebook-ban/13186354>.

96 Ibid. Google 'announced agreements with News Corp, Nine, Seven West, *The Guardian*, the ABC, and other Australian outlets': Gilbert + Tobin (n 94).

97 *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021* (Cth); Josh Frydenberg and Paul Fletcher, 'Parliament Passes News Media and Digital Platforms Mandatory Bargaining Code' (Joint Media Release, Department of the Treasury, 25 February 2021) <https://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/parliament-passes-news-media-and-digital-platforms>. See also Rita Matulionyte, 'News Media Bargaining Code: Australia Now Has Its Own Version of the Press Publisher's Right', *Kluwer Copyright Blog* (Blog Post, 24 March 2021) <http://copyrightblog.kluweriplaw.com/2021/03/24/news-media-bargaining-code-australia-now-has-its-own-version-of-the-press-publishers-right>.

98 Exposure Draft, Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020 (Cth) sch 1 pt 1 item 1.

99 Ibid.

them, through firstly a mediation process and, if negotiation fails, then through arbitration.[100]

It is unclear at this stage to what extent the Code will succeed in its goal of correcting the imbalance in bargaining power. Negotiation is still underway between government and data companies over what, exactly, the digital platforms should be paying for, with those platforms insistent that they should only pay for curation, expertise or paywalled content, rather than mere snippets or links, or items that are not 'news'. It appears that the large platforms are reaching agreements with news organisations independent of the mediation and arbitration process — and possibly, that they are striking bargains with larger organisations rather than the local and regional media who have arguably suffered most from the shift in advertising revenue.[101] A significant underlying problem concerns the 'information asymmetry', or the fact that 'it is currently very difficult for news media businesses to ascertain the value (especially the indirect value) that each of Google and Facebook derive from the use of news on their services'.[102] It is particularly difficult for small news media organisations to contest assertions from the large platforms that they derive little or no financial benefit from these uses of content. In any case, the Code has at least spurred digital platforms to pay something for the benefit they derive from their use of news content created by traditional media companies — although it is too early to say whether that payment reflects the true financial value of the benefit, let alone redresses the significant, and increasing, imbalance of power.

Thus, it is clear that the information-collecting capacities of large data companies raise significant legal issues, as well as broader concerns for the healthy functioning of democracy. The following parts of this article will consider the adequacy of legislative responses to these issues.

IV PUBLIC SURVEILLANCE

Firstly, however, we will consider some of the most significant recent concerns arising from public surveillance of the populace, by reference to the retention and sharing of data by government, the use of surveillance techniques such as facial recognition technology in criminal investigation, and the utilisation of national security rhetoric to justify incursions into privacy.

After World War II, the increased size and role of government, matched by significant technological advances, has allowed Australian governments to increase the amount of personal and commercially sensitive information collected.[103] This phenomenon accelerated in the 9/11 period, where the so-called

100 *Mandatory News Media Bargaining Code* (n 92) 7.

101 Gilbert + Tobin (n 94).

102 *Mandatory News Media Bargaining Code* (n 92) 8.

103 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia* (Report No 112, December 2009) 43.

war against terror led the government to increase their surveillance activities to identify suspected terrorists.[104] This was accompanied by a large volume of coercive anti-terrorism and surveillance laws, enacted at an unprecedented scale, speed and breadth — all in the name of national security.[105]

Widespread covert federal government surveillance is enabled by the *Telecommunications (Interception and Access) Act 1979* (Cth),[106] which empowers 'law enforcement, anti-corruption and national security agencies' to apply to the Attorney-General for warrants to 'intercept communications when investigating serious crimes and threats to national security',[107] or to a court or tribunal to approve warrants dealing with law enforcement activity.[108] From 1979, the Australian Security Intelligence Office ('ASIO') was also given the power to engage in electronic surveillance upon obtaining warrants issued by the Attorney-General, on the basis of a reasonable suspicion that a person was engaged in activities that could threaten national security.[109] The federal surveillance scheme on national security is thus based on warrants that are issued entirely within the executive by the Minister, rather than a more independent court or tribunal, meaning that it is a permissive scheme that would tend to lead to an increase in the numbers of warrants issued.

Further, the trend in Australia is towards the gradual and inexorable increase of surveillance powers at the expense of privacy protection, with the rhetoric of national security being deployed to justify the extension of powers. In 2011, legislation expanded the ability of ASIO to share intelligence with law enforcement and other intelligence agencies.[110] In 2015, legislation was enacted that required

104 Lachmayer and Witzleb (n 6) 748–50.

105 Simon Bronitt and Bernadette McSherry, *Principles of Criminal Law* (Lawbook, 4th ed, 2017) 1066–9; Christopher Michaelsen, 'Antiterrorism Legislation in Australia: A Proportionate Response to the Terrorist Threat?' (2005) 28(4) *Studies in Conflict and Terrorism* 321.

106 The states and territories also have legislation that operate alongside federal legislation which variously restrict the use of listening, optical, data and tracking surveillance devices: *Listening Devices Act 1992* (ACT); *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act 2007* (NT); *Invasion of Privacy Act 1971* (Qld); *Surveillance Devices Act 2016* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA).

107 Senate Legal and Constitutional Affairs References Committee, Parliament of Australia, *Comprehensive Revision of the Telecommunications (Interception and Access) Act 1979* (Report, March 2015) 9 [2.2] ('*Comprehensive Revision of the TIA Act*'), citing Attorney-General's Department (Cth), Submission No 26 to Senate Legal and Constitutional Affairs References Committee, *Inquiry into the Comprehensive Revision of the Telecommunications (Interception and Access) Act 1979* 3–4. See generally *Telecommunications (Interception and Access) Act 1979* (Cth) pts 2-2, 2-5.

108 *Comprehensive Review of the TIA Act* (n 107) 16.

109 *Australian Security Intelligence Office Act 1979* (Cth) s 26.

110 *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) sch 6. See generally Patrick F Walsh, 'Australian National Security Intelligence Collection Since 9/11: Policy and Legislative Challenges' in Randy K Lippert et al (eds), *National Security, Surveillance and Terror: Canada and Australia in Comparative Perspective* (Palgrave Macmillan, 2016) 51.

the mandatory retention of all Australians' metadata for two years and access by enforcement agencies without a warrant.[111] This has significant implications for privacy, as metadata is highly revealing both in terms of associations and also geographical movements (in case of mobile phones) and matters that an individual is thinking about (eg internet searches).

Most recently, the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) was passed by Parliament for the stated purpose of protecting national security and combating online crime through the dark web and anonymising technologies.[112] This Act increases the powers of law enforcement agencies by allowing them to issue three new types of warrants, including one that allows agencies to take control of an online account to gather information for an investigation, and modify and delete any data.[113] This ability to take control of and modify a person's social media account such as Facebook or Twitter involves wide-ranging incursions into personal privacy. Although there are safeguards built into the legislation, such as obtaining warrants through a judge or tribunal member, rather than warrants being approved solely within the executive, as well as judicial review and oversight by integrity bodies, an exceptional emergency authorisation procedure permits these activities without a warrant where there is an imminent risk of serious violence or substantial damage to property.[114] This legislation thus broadens the electronic surveillance powers of law enforcement authorities, while diminishing privacy protections.[115]

Another major issue is how public sector data is shared across government. The *Data Availability and Transparency Act 2022* (Cth) ('*DAT Act*') has been enacted, following the 2017 Productivity Commission's report into public sector data availability, which highlighted the value of public sector data sharing to improve

111 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 178, 187A–187C. Sections 187A–187C were inserted by *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) sch 1.

112 Revised Explanatory Memorandum, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) 14 [22]. The *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) updates the *Surveillance Devices Act 2004* (Cth) and *Telecommunications (Interception and Access) Act 1979* (Cth).

113 The Act introduces three new warrants: (1) data disruption warrants, which allow authorities to 'disrupt data by modifying, adding, copying or deleting'; (2) network activity warrants, which permit agencies to 'collect intelligence on serious criminal activity being conducted by criminal networks'; and (3) account takeover warrants, which let agencies take control of an online account (such as a social media account) to gather information for an investigation: Revised Explanatory Memorandum, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) 2–3 [6].

114 *Surveillance Devices Act 2004* (Cth) s 28(1A). The Act also contains other emergency authorisation procedures for accessing data: at ss 29(1A), 30(1A).

115 'Previous legislation, such as the *Telecommunications (Interception and Access) Act 1979* and the *Telecommunications Act 1997*, contained greater privacy protections': James Jin Kang and Jumana Abu-Khalaf, 'Facebook or Twitter Posts Can Now Be Quietly Modified by the Government under New Surveillance Laws', *The Conversation* (online, 7 September 2021) <https://theconversation.com/facebook-or-twitter-posts-can-now-be-quietly-modified-by-the-government-under-new-surveillance-laws-167263>.

economic and research activities and streamline service delivery.[116] The Act sets up a permissive data sharing scheme that allows users accredited by the National Data Commissioner to be provided with personal information by Commonwealth bodies ('data custodians') for the delivery of government services, to inform government policy and programs, and for research and development.[117] These accredited users can be from government, industry or the private sector,[118] meaning that the potential scope of data sharing is extremely broad, as private sector entities could be provided with personal data held by government.

The *DAT Act* does include certain privacy protections, including the prohibition on data sharing for law enforcement or national security purposes, as well as a data minimisation approach (ie 'only data that is reasonably necessary to achieve the [specified] project is shared').[119] To enhance transparency, a public register will be available, setting out 'what data is being shared and why, who is accessing data, and how it is being safely shared'.[120] Decisions of the National Data Commissioner are subject to judicial review and Ombudsman oversight.[121] Significant penalties apply to the unauthorised sharing of information, as well as unauthorised collection and use, which are criminal offences that may result in a maximum penalty of five years' imprisonment.[122] The Office of the Australian Information Commissioner noted that the Act overrides some protections to personal information afforded by the *Privacy Act 1988* (Cth) ('*Privacy Act*'), including 'existing secrecy provisions that ordinarily prevent the sharing of data, including personal information'.[123] Despite these concerns, overall it appears that the Act is proportionate and provides adequate privacy protections, supplemented by administrative law mechanisms for review.

In addition, to manage the global pandemic, COVID-related surveillance measures have been enacted. These include the contact tracing COVIDSafe app, which tracked proximity data with the aim of identifying those in contact with an infected person, which was given legislative basis through the *Privacy Amendment (Public Health Contact Information) Act 2020* (Cth). This app was voluntary and had

116 Productivity Commission, *Data Availability and Use* (Inquiry Report No 82, 31 March 2017); Explanatory Memorandum, Data Availability and Transparency Bill 2020 (Cth) 5 [1].

117 Explanatory Memorandum, Data Availability and Transparency Bill 2020 (Cth) 5–6 [7]–[11].

118 Ibid 6 [17].

119 Ibid 8 [35]. See also at 6, 8–9.

120 Senate Finance and Public Administration Legislation Committee, Parliament of Australia, *Data Availability and Transparency Bill 2020 [Provisions] and Data Availability and Transparency (Consequential Amendments) Bill 2020 [Provisions]* (Report, April 2021) 11–12 ('*DAT Bill and DATCA Bill Report*').

121 Ibid 25.

122 *Data Availability and Transparency Act 2022* (Cth) ss 14–14A.

123 Office of the Australian Information Commissioner, Submission No 16 to Senate Finance and Public Administration Legislation Committee, Parliament of Australia, *Inquiry into the Data Availability and Transparency Bill 2020* (12 March 2021) 3 [7], citing Data Availability and Transparency Bill 2020 (Cth) cl 23.

privacy protections, including the requirement for the data administrator to destroy the data at the end of the pandemic, and protection against private information about individuals being shared with law enforcement agencies.[124] Another large-scale mass surveillance mechanism is QR code tracking for those who attend public venues, mandated at the state and territory government level. Deep concerns have arisen about state police accessing this data on at least six occasions unrelated to criminal investigation.[125] We support the Australian Information Commissioner's recommendation that the police be banned from accessing QR code check-in data, apart from the purpose of COVID-19 contact tracing.[126] This limitation on the use of contact tracing data has been implemented in the Victorian pandemic legislation.[127]

In addition, facial recognition is being used by Australian police agencies, which have used a private facial recognition service called Clearview AI, which looks for a match with an uploaded image of a person's face through searching its database of several billion images collected from the web.[128] '[P]olice agencies initially denied they were using the service … until a list of Clearview AI's customers was stolen' and distributed online, showing both federal and state police.[129] No standards body exists to regulate or test the reliability or fitness of private technologies such as this, with the only testing apparently having been done in the United States by the company itself.[130] In late 2021, however, the Australian Information Commissioner, Angelene Falk, issued a determination that Clearview

124 See the now repealed *Privacy Act 1988* (Cth) pt VIIIA ('*Privacy Act*'); Explanatory Memorandum, Privacy Amendment (Public Health Contact Information) Bill 2020 (Cth) 21 [78], 28 [124]. See also Yee-Fui Ng and Stephen Gray, 'Wars, Pandemics and Emergencies: What Can History Tell Us about Executive Power and Surveillance in Times of Crisis?' (2021) 44(1) *University of New South Wales Law Journal* 227.

125 Graham Greenleaf and Katharine Kemp, 'Police Access to COVID Check-In Data Is an Affront to Our Privacy: We Need Stronger and More Consistent Rules in Place', *The Conversation* (online, 7 September 2021) <https://theconversation.com/police-access-to-covid-check-in-data-is-an-affront-to-our-privacy-we-need-stronger-and-more-consistent-rules-in-place-167360>.

126 Ibid.

127 See *Public Health and Wellbeing Act 2008* (Vic) s 165CD(1), which only authorises use or disclosure of contact tracing information 'for a public health purpose', 'in the performance of functions or the exercise of powers under [pt 8A of the Act]' or 'for a permitted purpose'. Use or disclosure is for a permitted purpose if there is consent, an 'imminent threat to life, health, safety or welfare' of at least one person, or for the 'purpose of taking enforcement action (including, but not limited to, issuing infringement notices or investigating or prosecuting an offence)' for either of the two offences under the Act (using or disclosing contact tracing information and providing false or misleading information): at s 165CD(2).

128 Jake Goldenfein, 'Australian Police Are Using the Clearview AI Facial Recognition System with No Accountability', *The Conversation* (online, 4 March 2020) <https://theconversation.com/australian-police-are-using-the-clearview-ai-facial-recognition-system-with-no-accountability-132667>.

129 Ibid, citing Ryan Mac, Caroline Haskins and Logan McDonald, 'Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart and the NBA', *Buzzfeed News* (online, 28 February 2020) <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement>.

130 Mac, Haskins and McDonald (n 129).

AI had breached the Australian *Privacy Act*, ordering them to cease collecting facial images and biometric templates, and to destroy those it had already collected.[131] It is unclear whether this has yet occurred or whether police are no longer using the service.

Following a Council of Australian Governments ('COAG') agreement in 2017, the federal government embarked on a process designed to legalise the collection and sharing of facial images and other identity information among government agencies Australia-wide.[132] It might even have legalised sharing with private organisations.[133] Known as the 'identity matching laws', the package of legislation aimed to set up a national 'hub' for the sharing of such information, under the scrutiny of the Department of Home Affairs. Its aims included identifying missing individuals, including in times of disaster or emergency, as well as combatting identity crime and promoting community safety.[134] While it appears that the proposed legislation has now lapsed, in July 2021 the federal government announced an intergovernmental agreement on data sharing, which 'commit[s] all governments to use best endeavours to share data between jurisdictions as a default position; where it can be done securely, safely, lawfully and ethically'.[135]

It is clear that police use of FRT in investigating crime or identifying suspects raises a significant set of privacy and human rights issues. The scheme could be used to identify any Australian, regardless of whether they were suspected of a crime. The Australian Human Rights Commission ('AHRC') has argued that the facial-matching software used could discriminate against particular racial or gender groups.[136] In 2021, the AHRC's final report *Human Rights and Technology* recommended a moratorium on the use of FRT until legislation can be passed regulating its use and expressly protecting human rights.[137] We argue that FRT needs to be carefully deployed in high-stakes situations that impact upon a person's fundamental rights of life, liberty or property, such as in criminal investigations in

131 *Commissioner Initiated Investigation into Clearview AI Inc* [2021] AICmr 54, [240]–[242].

132 Sarah Moulds, 'Who's Watching the "Eyes"? Parliamentary Scrutiny of National Identity Matching Laws' (2020) 45(4) *Alternative Law Journal* 266, 267, citing Council of Australian Governments, *Intergovernmental Agreement on Identity Matching Services* (5 October 2017) <https://federation.gov.au/sites/default/files/about/agreements/iga-identity-matching-services.pdf>.

133 Department of Parliamentary Services (Cth), *Bills Digest* (Digest No 21 of 2019–20, 26 August 2019) 3. See also Moulds (n 132) 267.

134 Moulds (n 132) 267.

135 National Cabinet, *Intergovernmental Agreement on Data Sharing between Commonwealth and State and Territory Governments* (9 July 2021) 2 <https://federation.gov.au/sites/default/files/about/agreements/iga-on-data-sharing-signed.pdf>.

136 Moulds (n 132) 268, citing Australian Human Rights Commission, 'Identity Matching Bills Threaten Our Rights' (Media Release, 3 May 2018) <https://humanrights.gov.au/about/news/identity-matching-bills-threaten-our-rights>.

137 Australian Human Rights Commission, *Human Rights and Technology* (Final Report, 2021) 115–16, 120 ('*Human Rights and Technology*').

order to avoid wrongful arrests and detention.[138] Accordingly, FRT should only be deployed when the accuracy of the technology is confirmed for its intended purpose, and when there are strong legislative guidelines regulating its use, as well as the ability for individual appeals over errors from the use of this technology.

The extensive national security and surveillance laws, combined with weak privacy protections, have enabled the government to strategically utilise national security laws to justify significant interferences with privacy. For example, the Australian Federal Police raided a News Corp journalist's residence and the ABC's Ultimo premises under a warrant.[139] Upon a legal challenge, the High Court held that the warrant authorising the raids was invalid, although on the narrow basis of the content of the warrant, rather than any substantive privacy right.[140] In particular, the High Court majority (Kiefel CJ, Bell and Keane JJ, joined by Nettle J) held that an injunction to compel the return or destruction of the unlawfully seized phone data was neither available nor appropriate,[141] and the Court did not venture into expanding equity or tort law to recognise any common law privacy rights.[142] This shows the limitation of the Australian privacy laws, as will be discussed in further detail in Part V below. At a broader level, the utilisation of national security laws by government to attack journalists endangers press freedom, which is a fundamental tenet of a healthy democracy.

To sum up, public surveillance experienced an explosion following the 9/11 incident, leading to widespread coercive laws justified on the basis of national security, with a general trend towards increasing surveillance powers by law enforcement authorities at the expense of privacy protections. This has been supplemented by increased data sharing in government, as well as pandemic-related surveillance in terms of location and proximity tracking. The use of facial recognition technologies has raised concerns in terms of privacy and human rights

138 Daniel E Ho et al, 'Evaluating Facial Recognition Technology: A Protocol for Performance Assessment in New Domains' (2021) 98(4) *Denver Law Review* 753, 754–6.

139 The Australian Federal Police ('AFP') executed a search warrant at the residence of News Corp journalist Annika Smethurst and at the ABC's Ultimo premises. The AFP claimed both searches related to 'separate allegations of publishing classified material, contrary to provisions of the *Crimes Act 1914*, which is an extremely serious matter that has the potential to undermine Australia's national security': Australian Federal Police, 'AFP Statement on Activity in Canberra and Sydney' (Media Release, 5 June 2019) <https://www.afp.gov.au/news-media/media-releases/afp-statement-activity-canberra-and-sydney>.

140 The High Court found that the warrant was invalid as it misstated the substance of s 79(3) of the *Crimes Act 1914* (Cth) and failed to state the offence to which the warrant related with sufficient precision: *Smethurst v Commissioner of Police* (2020) 272 CLR 177, 198–9 [20]–[21] (Kiefel CJ, Bell and Keane JJ, Gageler J agreeing at 227 [115], Nettle J agreeing at 236 [142], Gordon J agreeing at 246 [166]–[167]), 265 [225] (Edelman J) ('*Smethurst*'). However, the High Court did not make an order for the destruction of the documents seized: at 221–3 [99]–[104] (Kiefel CJ, Bell and Keane JJ, Nettle J agreeing at 245 [163]).

141 *Smethurst* (n 140) 221–3 [99]–[104] (Kiefel CJ, Bell and Keane JJ), 244–5 [160]–[163] (Nettle J).

142 Ibid 217–18 [86]–[90] (Kiefel CJ, Bell and Keane JJ), 271–3 [240]–[244] (Edelman J). See also Rebecca Ananian-Welsh and Joseph Orange, 'The Confidentiality of Journalists' Sources in Police Investigations: Privacy, Privilege and the Freedom of Political Communication' (2020) 94(10) *Australian Law Journal* 777.

issues. A major concern about this extensive range of laws that cover many aspects of individual activity is that they have been interpreted broadly or utilised strategically to affect individual rights and freedoms. Thus, it is necessary to consider what legal reforms are required to balance the rights of individuals against the incursions of the state.

V LAW REFORM PROPOSALS

One possible avenue for the improved regulation of public and private surveillance, and particularly data surveillance, is through privacy law. Information privacy laws are a logical starting point for addressing the problems of surveillance because they deal with the issue at its source — ie the collection and processing of personal information. However, Paterson and McDonagh have identified 'key limitations' in the capacity of privacy law 'to address the [challenges] posed by Big Personal Data'.[143] The *Privacy Act*, which contains a set of information privacy principles imposing limitations, including on the collection, use and disclosure of personal information, is limited in its coverage of private sector organisations, particularly small businesses, and also political parties.[144] Its coverage is limited to personal information.[145] The limitations on use and disclosure are based on what is 'reasonably necessary', rather than on the data subject's consent.[146] While consent is required where the information is sensitive, the difficulties with consent in the context of Big Data collection make this requirement very difficult to monitor or administer.[147]

Further, there are issues of group privacy, where groups are analysed based on shared characteristics and then individuals are dealt with based on their membership of those groups.[148] Another issue is that data that is notionally de-identified and therefore not protected is potentially re-identifiable in the context of Big Data.[149] In addition, a person may not be identifiable per se but nevertheless subject to manipulation.[150] Furthermore, although data protection laws offer additional protection for characteristics (eg ethnicity, sexual orientation), Big Data

143 Paterson and McDonagh (n 9) 2.

144 *Privacy Act* (n 124) s 6C. See also ibid 9.

145 Paterson and McDonagh (n 9) 10–12. See Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30(4) *Philosophy and Technology* 475.

146 Paterson and McDonagh (n 9) 13–14.

147 See above n 52 for discussion of the issues with 'click-wrap' consent. See also ibid 14–15.

148 Mittelstadt (n 145) 476. See the discussion of group privacy in Paterson and McDonagh (n 9) 10, quoting Andrej Zwitter, 'Big Data Ethics' (2014) 1(2) *Big Data and Society* 1, 4.

149 Paterson and McDonagh (n 9) 11.

150 Ibid 7.

allows for use of proxies for these attributes, thus avoiding this additional protection.[151]

In practical terms, the privacy principles are of limited value given that they are not enforceable in court except against public sector agencies, and are governed by a regulatory body, the Office of the Australian Information Commissioner, which is 'relatively small and poorly resourced'.[152]

Australian privacy law is principles-based rather than providing for a general right to privacy for individuals.[153] As a result, an individual's privacy is not effectively protected because privacy legislation provides 'very limited civil redress', is limited in scope (as discussed above), and only protects privacy of information, and not 'territorial, communications and bodily privacy'.[154] Consequently, privacy invasions are in effect pursued under a hodgepodge of other laws, such as tortious actions of trespass to the person, trespass to land and nuisance, equitable actions such as breach of confidence, and legislative and common law protections against surveillance.[155] However, there are significant gaps in the current laws, which do not provide protection from unauthorised and serious intrusions into a person's private activities and do not sufficiently protect against technological advances that 'facilitate new types of invasion into personal privacy', nor 'provide a remedy for intentional infliction of emotional distress which does not amount to psychiatric illness'.[156] In addition, there is 'no tort or civil action for harassment, nor is there sufficient deterrence against "cyber-harassment"'.[157]

To address the deficiencies in privacy protection in Australia, one possibility of reform, extensively discussed in Australia in recent years, is the introduction of a statutory cause of action for invasion of privacy. A series of law reform commissions and parliamentary inquiries have concluded that Australian law ought to provide a cause of action for an individual who suffers a serious,

151 Mittelstadt (n 145) 479, 488.

152 See discussion in Bartlett, 'Beyond Privacy' (n 2) 100.

153 Justin Penna, 'Is Australia's Statutory Regime for Privacy Protection Fit for the Purpose of Regulating Public Agencies in the Era of Big Data? An Examination into the Data Availability and Transparency Legislation' [2021] *University of New South Wales Law Journal Student Series* 12:1–17, 2–3. See Carolyn Doyle and Mirko Bagaric, *Privacy Law in Australia* (Federation Press, 2005) 5.

154 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Final Report No 123, June 2014) 47–51, 53, 60–1 ('*Serious Invasions of Privacy in the Digital Era*').

155 Ibid 51–2 [3.50].

156 Ibid.

157 Ibid.

unjustified invasion of privacy.[158] In 2001, in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* ('*Lenah*'),[159] the High Court 'left the door open for a common law tort of interference with privacy',[160] and subsequent lower court decisions have labelled the action a 'logical and desirable step'.[161] In 2014, an Australian Law Reform Commission ('ALRC') report, *Serious Invasions of Privacy in the Digital Era*, detailed the elements of a statutory cause of action.[162]

It is difficult to argue with the proposition that such a tort should be enacted to cover the misuse of private information, or the violation of seclusion, provided a seriousness threshold is satisfied. Such a reform was recommended by the ACCC's *Digital Platforms Inquiry* report,[163] with the Commonwealth government responding that it would review the *Privacy Act* to consider whether a broader reform of Australian privacy law was necessary.[164] In February 2023, the government published the final report from its review of the effectiveness of the framework in the *Privacy Act* to protect personal information, which recommended, amongst other things, that a tort of invasion of privacy be introduced into Australian law.[165] This statutory tort would empower the courts to award damages, including damages for emotional distress where private information was disclosed in breach of confidence.[166] The ALRC proposed that the statutory tort should enable plaintiffs to seek a very wide range of remedies, including some innovative remedies, such as an order to publish a correction of false information, or an order that the defendant must apologise.[167] Also in 2021,

158 See, eg, Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy* (Report No 11, 1979) 121–2 [230]–[232]; New South Wales Law Reform Commission, *Invasion of Privacy* (Report No 120, April 2009) 17 [4.14]; Victorian Law Reform Commission, *Surveillance in Public Places* (Final Report No 18, 12 August 2010) 147 [7.113], [7.115]; Department of the Prime Minister and Cabinet, 'A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy' (Issues Paper, September 2011).

159 (2001) 208 CLR 199 ('*Lenah*'). See generally Gligorijevic (n 55).

160 Gligorijevic (n 55) 673. See also Normann Witzleb, 'A Statutory Cause of Action for Privacy? A Critical Appraisal of Three Recent Australian Law Reform Proposals' (2011) 19(2) *Torts Law Journal* 104, 106 ('A Statutory Cause of Action for Privacy').

161 *Grosse v Purvis* (2003) Aust Torts Reports ¶81-706, 64,187 [442] (Skoien J). See Jim Micallef and Madeleine James, 'All Talk, No Cause of Action: Where to Next for an Australian Cause of Action for Serious Invasion of Privacy?' (2020) 39(1) *Communications Law Bulletin* 32, 33.

162 *Serious Invasions of Privacy in the Digital Era* (n 154). See also Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 3, 2567–77 [74.129]–[74.168].

163 *Digital Platforms Inquiry* (n 32) 493.

164 *Regulating in the Digital Age* (n 91) 18.

165 Attorney-General's Department, Australian Government, *Privacy Act Review* (Report, 2022) <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>.

166 This is outlined in recommendation 13-1: *Serious Invasions of Privacy in the Digital Era* (n 154) 13.

167 This is outlined in recommendations 12-10 and 12-11: ibid.

the AHRC supported a statutory cause of action for serious invasion of privacy as a 'barrier to intrusive, wide-scale surveillance'.[168]

However desirable, such a reform is unlikely to provide an effective remedy for the broader types of everyday data surveillance and collection discussed above. It only covers serious invasions of privacy, not the routine harvesting of personal information from social media 'likes' and preferences, and its sale to third parties, nor does it deal with government surveillance. It places the onus on the plaintiff, an extremely difficult burden to satisfy given the imbalance of power existing between the ordinary consumer and the 'Big Data' harvesters. Plaintiffs also face further difficulties due to the high costs of litigating and the difficulties of establishing loss.

A further possibility sometimes discussed, either as an alternative or a complement to a statutory tort of privacy, is the expansion of equitable principles, specifically the law of breach of confidence. This action, which has been most frequently used in England, provides a remedy for the unauthorised disclosure of confidential information, in circumstances where an obligation of confidence exists.[169] It is 'a form of unconscionable conduct, akin to a breach of trust'.[170] It has been interpreted in a relatively restrictive way in Australia, with the High Court in *Smethurst v Commissioner of Police* reiterating the finding in *Lenah* that the circumstances in the earlier case did not establish an equitable right to a remedy protecting privacy.[171] There have been occasional hints that the Australian law on breach of confidence might be expanded: for example, the Victorian Court of Appeal's decision in *Giller v Procopets* to award damages for distress in relation to a claim of breach of confidence as an equitable doctrine,[172] is a promising precedent towards individuals claiming compensation for the misuse of private information.[173] However, expansion in the direction of a broader equitable principle protecting privacy has not so far been forthcoming in Australian case law.

Gligorijevic argues that a common law tort of invasion of privacy is more suitable than equitable remedies for the types of harm at issue in *Lenah*, suggesting that 'the fashioning of compensatory damages in equity for non-tortious dignitary harm

168 *Human Rights and Technology* (n 137) 123.

169 *Campbell v MGN Ltd* [2004] 2 AC 457, 464–5 [13]–[14] (Lord Nicholls) ('*Campbell*').

170 Ibid 464 [13].

171 *Smethurst* (n 140) 215 [81] (Kiefel CJ, Bell and Keane JJ), discussing *Lenah* (n 159). See also Gligorijevic (n 55) 708.

172 (2008) 24 VR 1. This case concerned a plaintiff who sought damages for the distress caused by the unauthorised showing of a private sex tape by her former partner to her family, friends and employer.

173 See generally Normann Witzleb, '*Giller v Procopets*: Australia's Privacy Protection Shows Signs of Improvement' (2009) 17(2) *Torts Law Journal* 121.

or distress is problematic'.[174] However, the ALRC has recommended that legislation should be enacted confirming that an action for breach of confidence allows compensation to be awarded for emotional distress arising from the misuse of private information.[175] We will argue for an expansion of equitable doctrine based on the notion of a data fiduciary in Part VI below.

Another approach to privacy protection is through public law. In this regard, the data protection laws of the European Union provide an interesting possible model for Australia. The Court of Justice of the European Union held that a directive enforcing a blanket retention of metadata by Internet Service Providers ('ISPs') for two years infringed the right to privacy, and was therefore invalid under arts 7, 8 and 52(1) of the *Charter of Fundamental Rights of the European Union* ('*EU Charter*').[176] A fundamental reason for the breach was the fact that the metadata had to be retained for two years, and was required to be accessible to and processed by competent national authorities.[177] This derogated from directives that required the confidentiality of data, and the obligation to erase or anonymise data where no longer necessary.[178] This has been recently reinforced by the Grand Chamber of the Court of Justice of the European Union, which has ruled that the *e-Privacy Directive*[179] and *EU Charter* prevent national law from enabling the bulk retention and transmission of traffic and location data, even for the purposes of national security.[180] However, this was qualified by the Court noting that EU law does not prohibit indiscriminate data retention measures where there are proven serious threats to national security, although bulk data can only be retained during a strictly necessary period and the decision to retain the data must be subject to review by a court or an independent administrative body.[181] By contrast, as discussed above,

174 Gligorijevic (n 55) 710, citing JD Heydon, MJ Leeming and PG Turner, *Meagher, Gummow and Lehane's: Equity Doctrines and Remedies* (LexisNexis Butterworths, 5th ed, 2015) 882–3 and PG Turner, 'Privacy Remedies Viewed through an Equitable Lens' in Jason NE Varuhas and NA Moreham (eds), *Remedies for Breach of Privacy* (Hart Publishing, 2018) 265.

175 This is outlined in recommendation 13-1: *Serious Invasions of Privacy in the Digital Era* (n 154) 13. See also Gligorijevic (n 55) 708.

176 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (Court of Justice of the European Union, C-293/12, C-594/12, ECLI:EU:C:2014:238, 8 April 2014) [69], citing *Charter of Fundamental Rights of the European Union* [2012] OJ C 326/391, arts 7, 8, 52(1).

177 Ibid [32].

178 Ibid.

179 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* [2002] OJ L 201/37.

180 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* (Court of Justice of the European Union, C-623/17, ECLI:EU:C:2020:790, 6 October 2020) [82]; *La Quadrature du Net v Premier Ministre* (Court of Justice of the European Union, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791, 6 October 2020) [137], [168] ('*La Quadrature*'). See also Monika Zalnieriute, 'A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union' (2022) 85(1) *Modern Law Review* 198.

181 *La Quadrature* (n 180) [168].

the retention of metadata for an equivalent period without a warrant has been legislated without legal challenge in Australia.[182]

In addition, in the UK, the use of facial recognition technology has been successfully challenged on a human rights basis in *R (Wood) v Commissioner of Police of the Metropolis*, with the Court of Appeal holding that the police surveillance of a campaigner against the arms trade was in breach of art 8 of the *European Convention on Human Rights*.[183] In addition, in the case of *R (Bridges) v Chief Constable of South Wales Police*, the Court of Appeal accepted that South Wales Police's use of facial recognition technology was an interference with Bridges' privacy rights under art 8(1), and was not 'in accordance with the law' for the purpose of art 8(2).[184] It also considered that the use of the technology was in breach of public sector equality duties, in that the police had not done everything reasonable to be satisfied that the software used did not have a racial or gender bias.[185]

Although Australian police utilise similar facial recognition technology, none of these challenges would be possible under Australian law, which lacks a framework of explicit human rights and privacy protection. This shows the strength of a rights-based interpretation of privacy principles compared to Australia's framework, which lacks robust rights protections. As Australia lacks the foundational human rights framework to support privacy protections, this is a less feasible avenue in Australia compared to a statutory cause of action or an expansion of equitable principles.

Another possible reform, which supplements the other proposed reforms, might be the adoption in Australia of law similar to the *General Data Protection Regulation* ('*GDPR*'), which began operation in the European Union in May 2018.[186] The *GDPR* contains a broader definition of personal data, applying to information that can be directly or indirectly linked to a particular person.[187] While a data collector may have a legitimate interest in processing or using personal data, that interest may be 'overridden by the interests or fundamental rights and freedoms of the data

182 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 178, 187A–187C. Sections 187A–187C were inserted by *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) sch 1.

183 [2010] 1 WLR 123, 154–5 [85]–[90] (Dyson LJ), 156–7 [96]–[97] (Lord Collins), citing *Human Rights Act 1998* (UK) sch 1. See generally *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 Freedoms, Amending the Control System of the Convention*, opened for signature 13 May 2004, CETS No 194 (entered into force 1 June 2010).

184 [2020] 1 WLR 5037, 5081 [210] (Etherton MR, Sharp P and Singh LJ).

185 Ibid 5079–80 [201]. See also discussion in *Human Rights and Technology* (n 137) 118.

186 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 ('*GDPR*').

187 See discussion and references in Paterson and McDonagh (n 9) 16.

subject'.[188] Where the data is sensitive, the *GDPR* requires explicit consent, while the *Privacy Act* does not require consent to be explicit.[189] Nevertheless, the difficult issue remains of how informed 'consent' can be given where even the data collector cannot predict in advance how the information will be used. This arguably has the effect that the *GDPR* has limited power to restrict the second and third-order products of personal data, or data mining.[190] According to Paterson and McDonagh, while the adoption of rules that are akin to those of the *GDPR* in Australia might 'go some way towards addressing' the challenges of Big Data, the regime does 'not address the significant issue of group privacy' (ie individuals who are defined by membership of some group), or 'fully address the issue of re-identification of data', nor does it fully address the shortcomings of the consent model.[191]

VI AN ADDITIONAL APPROACH: INFORMATION FIDUCIARY

While the proposals discussed above are useful reforms, they do not overcome all of the problems associated with 'Big Data' surveillance and collection. An additional promising reform, we believe, and one little discussed in Australia so far, is the notion of the 'information fiduciary'. This proposal has been most extensively elaborated upon in the United States, where Balkin, amongst others, has argued that 'many online service providers and cloud companies who collect, analyze, use, sell and distribute information should be seen as information fiduciaries towards their customers and end-users'.[192] The fiduciary relationship, Balkin argues, arises from the special power of data collectors over others, giving rise to 'special duties to act in ways that do not harm the interests of' those whose data they collect.[193] The relationship is based on trust and confidence — in other words, the type of relationship traditionally protected in equity.[194] As Balkin points out, 'certain kinds of information constitute matters of private concern not because of their *content*, but because of the *social relationships* that produce them'.[195] This information fiduciary concept could apply to both public and private digital data collectors and online service providers.

188 *GDPR* (n 186) art 6(1)(f).

189 Ibid art 9(2)(a). Cf *Privacy Act* (n 124) s 6 (definition of 'consent'). See Paterson and McDonagh (n 9) 18.

190 Bartlett, 'Beyond Privacy' (n 2) 100.

191 Paterson and McDonagh (n 9) 30.

192 Balkin (n 18) 1186. In fact, Balkin is not the first to suggest the notion of an information fiduciary: see, eg, Jerry Kang et al, 'Self-Surveillance Privacy' (2012) 97(3) *Iowa Law Review* 809, 831–2 and other sources cited in Balkin (n 18) 1221.

193 Balkin (n 18) 1186.

194 Ibid 1187.

195 Ibid 1205 (emphasis in original). See generally William von Hippel, *The Social Leap: The New Evolutionary Science of Who We Are, Where We Come from, and What Makes Us Happy* (Harper Wave, 2018).

At first sight, the relationship between the data collector and the individual may not seem comparable to the type of relationship traditionally recognised as fiduciary — typically, a professional handling money or property for a client. However, a traditional fiduciary also handles sensitive information,[196] obtained in the course of their relationship. The individual, or the person to whom fiduciary duties are owed, is likely to be 'uninformed, vulnerable, and dependent' in that relationship,[197] and needs to be able to trust the fiduciary. Because of this vulnerability, it is easy for the fiduciary to abuse that trust.[198]

It is true that the relationship between individual and digital platform is not identical to that between professional and client. As Balkin points out, this relationship does not require the same degree of obligation and loyalty as would be required, for example, of a doctor or lawyer, or a person managing an estate.[199] Nevertheless, it does require that the data collector or information fiduciary not betray the trust implicitly reposed in them by the individual releasing data for their profit — in other words, they should not 'use the data in unexpected ways to the disadvantage of people who use their services or in ways that violate some other important social norm'.[200] In addition, there is an imbalance of power for certain vulnerable segments of the population, such as children, the elderly or those with medical issues.

The legal notion of a fiduciary relationship has significant advantages over other vehicles, such as a tort of invasion of privacy. In particular, the fiduciary relationship places the onus on the data harvester or collector to act in a trustworthy manner.[201] The individual is not placed in the difficult position of having to prove their privacy has been invaded, where it may not be clear precisely what the data harvester has done, or what benefit they have gained, as the burden of proof would be on the fiduciary.[202] It should be possible to clarify the precise nature of the duties owed, placing the onus on the data harvester to prove that the duties are not breached, thus imposing 'new expectations that data custodians themselves address (assess, avoid and mitigate residual risks) of unfair or unreasonable impacts upon individuals'.[203] In addition, as Bartlett points out, the notion of an information fiduciary is consistent with the putative values of the Big Data

196 Balkin (n 18) 1207.

197 Ibid 1215.

198 Ibid 1217.

199 Ibid 1221.

200 Ibid 1227.

201 Bartlett, 'Beyond Privacy' (n 2) 104.

202 As Bartlett points out, this is the product of the 'information asymmetry incumbent in the data economy that makes genuine consent extremely difficult to determine': ibid.

203 Peter Leonard, 'Data Privacy in a Data- and Algorithm-Enabled World' (2020) 17(3) *Privacy Law Bulletin* 43, 46.

harvesters themselves, particularly the 'idea that they should be trusted with your data'.[204]

In addition, although without labelling it as such, Australian law has already taken steps towards regulating the behaviour of 'Big Data' in a manner consistent with the notion of an information fiduciary. The notion of a fiduciary stems from the imbalance of power between individual and fiduciary, and the vulnerability of the individual in that relationship. The imbalance between traditional media platforms and the data collector has been well recognised in recent Australian debate. The *Digital Platforms Inquiry* devotes much of its considerable length and extensive research to establishing precisely this point.[205] As noted above, the Commonwealth government's *News Media Bargaining Code*, passed in February 2021, was developed pursuant to the recommendations of this inquiry, with a similar purpose of addressing power imbalances between traditional media and the digital platforms, including particularly the 'information asymmetries' between the two.[206] Thus, the imbalance of power is recognised as stemming from the enormous amounts of data collected by the digital platforms, placing news organisations in a vulnerable position when it comes to negotiating agreements — a situation with close parallels to the position of the 'information fiduciary' described above.

Traditional news media are in a somewhat different position to individuals whose data is harvested, in that they are at least alert to the issue of data collection and are aware of their revenue loss. Individuals are likely to have limited awareness of the issue, and even less ability to discern the extent of profit gained at their expense.[207] Like individuals, traditional news media are dependent on online platforms for the services they provide and do not have a real alternative to dealing with platforms operating in highly concentrated markets. However, their vulnerability is a different one: it is not their data that is collected, but instead the online platforms control access to consumers. It is conceivable that the notion of a 'data labor union', advocated for in the United States by Posner and Weyl,[208] may help address this situation. Essentially this idea involves individuals being banded together in a group or union to manage and represent their interests in their personal data and negotiate with technology platforms. Such negotiations would need to be consistent with principles similar in some respects to those in the *News Media Bargaining Code*, designed to ensure that no advantage is taken of the data controller's position of power.

204 Bartlett, 'Beyond Privacy' (n 2) 104.

205 See, eg, *Digital Platforms Inquiry* (n 32) 8–9, concerning Facebook and Google's extensive market power.

206 *Mandatory News Media Bargaining Code* (n 92) 1, 8.

207 See Bartlett, 'Beyond Privacy' (n 2) 103.

208 Eric A Posner and E Glen Weyl, *Radical Markets: Uprooting Capitalism and Democracy for a Just Society* (Princeton University Press, 2019) 242–3. See also discussion in Bartlett, 'Beyond Privacy' (n 2) 105.

The equitable remedy we are arguing for in proposing the information fiduciary principle can be analogised to the broader remedy available in the United Kingdom, which is derived from the traditional action of breach of confidence.[209] The UK 'extended' action of breach of confidence protects against disclosures of private information.[210] Thus, an expanded equitable doctrine in Australia is congruent with this expansion observed in the UK. The information fiduciary principle might also be consistent with laws beginning to be enacted in other jurisdictions, such as the concept of the 'guardian data fiduciary' enshrined in a proposed Digital Personal Data Protection Bill in India.[211] We suggest that the equitable concept of the information fiduciary will operate alongside the *Privacy Act* and any proposed causes of action for privacy.

Given the limitations of Australia's fiduciary principles and the confused nature and scope of various causes of actions and remedies at common law,[212] we suggest the notion of an information fiduciary would need to be given legislated form. The legislation might define those who are subject to the duties of a fiduciary, including particularly the Big Data companies and government organisations. The 'Big Data' companies to be subjected to the duties of an information fiduciary could be online service providers that possess personal information, such as 'social media companies like Facebook, search engines like Google and service platforms like Uber'.[213] Government organisations to be subject to the duties would be the data custodians currently subject to the *DAT Act*, discussed above, which are Commonwealth bodies that control public sector data.[214] In terms of national security and law enforcement bodies, given the need for these agencies to balance broader national security considerations with individual data protection, there are arguments to include limitations for these organisations. However, there should be adequate legislative safeguards for individuals in the use of their data by these agencies to prevent abuse in terms of data minimisation, judicial review and scrutiny by oversight bodies.

209 *Campbell* (n 169) 464–5 [13]–[15] (Lord Nicholls), 472–3 [46]–[51] (Lord Hoffman).

210 Ibid 473 [51] (Lord Hoffman). Cf *Ashburton v Pape* [1913] 2 Ch 469.

211 Digital Personal Data Protection Bill 2022 (India) cl 10, which states that a 'Data Fiduciary shall not undertake such processing of personal data that is likely to cause harm to a child' or 'undertake tracking or behavioural monitoring of children or targeted advertising directed at children'. For further discussion of the now withdrawn Personal Data Protection Bill 2019 (India), see also Peter G Leonard, 'Notice, Consent and Accountability: Addressing the Balance between Privacy Self-Management and Organisational Accountability' (Paper, Data Synergies, June 2020) 38–9 [4.1] <https://www.oaic.gov.au/__data/assets/pdf_file/0003/2010/notice-and-consent-paper-for-oaic.pdf.pdf>.

212 Generally, a fiduciary relationship arises where one party undertakes to act in the interests of another 'in the exercise of a power or discretion which will affect the interests of that other person in a legal or practical sense': *Hospital Products Ltd v United States Surgical Corporation* (1984) 156 CLR 41, 97 (Mason J). Accepted fiduciary relationships include those of 'trustee and beneficiary, agent and principal, solicitor and client, employee and employer, director and company, and partners': at 96.

213 Balkin (n 18) 1232.

214 See above nn 116–18 and accompanying text.

The legislation could then define the nature of the duties to be imposed on the data fiduciary. The precise nature of the duties would need to be flexible, depending on the nature of the relationship, but would include classic fiduciary duties, such as a duty of care 'in terms of safely storing, securing, deleting, analyzing, and presenting' data, a duty of confidentiality in not disclosing the data of the beneficiary, a duty to avoid improper use of position and improper use of the beneficiary's data, a duty to act in the best interests of the beneficiary, and a duty to avoid conflicts of interest with the beneficiary.[215] The duties would also likely include a requirement of obtaining free, voluntary and informed consent to the uses of data, as well as a requirement to negotiate agreements fairly. The legislation might also require the data controller, or fiduciary, to identify how they comply with privacy obligations, which is consistent with the principle of accountability enshrined in global privacy and data protection law.[216] It would also provide for remedies, such as compensatory damages (including for intentional infliction of emotional distress), injunctions and declarations.[217]

The notion of a data fiduciary, we suggest, provides a useful unifying principle for various measures already undertaken, as well as an alternative model for carrying into effect 'what good practice looks like, how it is given effect … and how to balance incentives for good behaviour and sanctions for unacceptable behaviour'.[218] It represents a useful way, not to put the genie of Big Data surveillance back in the bottle, but to ensure that it remains as consistent as possible with the vision of the early pioneers of the internet, as a servant of human agency and individual choice, rather than a master, whose true loyalties lie elsewhere.

VII CONCLUSION

In 1883, in light of the modern technology of the time, the instantaneous photograph, Warren and Brandeis first conceptualised the right to privacy in the *Harvard Law Review*, which they called the 'general right of the individual to be let alone'.[219] In searching for a new foundation of this common law right of privacy, they grasped at and distinguished it from contract law (such as trade secrets), property and copyright law,[220] but suggested that remedies for invasion of

215 Kang et al (n 192) 832; Balkin (n 18) 1207–8.

216 Teresa Troester Falk, 'The Concept of "Accountability" as a Privacy and Data Protection Principle', *CPO Magazine* (online, 19 February 2016) <https://www.cpomagazine.com/data-privacy/concept-accountability-privacy-data-protection-principle>.

217 This is consistent with the remedies proposed by a potential statutory cause of action for privacy: Witzleb, 'A Statutory Cause of Action for Privacy' (n 160) 107.

218 Leonard, 'Data Privacy in a Data- and Algorithm-Enabled World' (n 203) 47.

219 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193, 205.

220 Ibid 207–13.

privacy could be obtained through an action in tort, or injunctions in limited cases, or protected legislatively via criminal law in the case of serious breaches.[221]

More than a century later, the impetus for privacy protection is stronger than ever before. Advances in Big Data analytics have enabled both private corporations and governments to greedily harvest personal and sensitive information with ever-alarming volumes and velocities. Yet the law of privacy, particularly in Australia, is still limping along, searching for a firmer foundation.

Australian privacy law, being principles-based with multiple exclusions, does not provide sufficient individual protection against privacy incursions. These limitations have allowed the widespread surveillance in both the public and private sector without strong safeguards. The rhetoric of national security has been a trump card that has enabled widespread public surveillance, while the power of Big Data harnessed by multinational corporations has enabled them to collect vast volumes of private and sensitive individual data.

Although the human rights-based protections of privacy as adopted in the UK and in the EU possess distinct attractions, these are less likely to be adopted in Australia, which lacks a foundational framework for rights protections. Accordingly, we argue that a complementary approach involving legislated causes of actions for privacy and the expansion of equitable remedies via the principle of an information fiduciary proposed by Balkin provides a more tenable basis for privacy protections in Australia. The information fiduciary principle explicitly recognises the power and information asymmetry between a data collector, whether the government or a large corporation, compared to an uninformed individual, and imposes an active duty on data collectors to act in the best interests of the data subjects, who are in a more vulnerable position in terms of understanding how their data is used. We contend that this expansion of equitable principles provides a useful additional mode of protection of personal and sensitive information in a digital age.

In an algorithmic society, where great power resides in the collection and utilisation of personal data by government and private corporations alike, it is imperative that the diluted privacy laws in Australia evolve to better protect individuals against the advancing juggernaut of Big Data and AI surveillance.

221 Ibid 219.