Normann Witzleb

Responding to Global Trends? Privacy Law Reform in Australia

A Introduction

This contribution explores the extent to which Australian privacy law reform in the early 2020s engages with, and is influenced by, global developments and trends. It has a particular focus on the major (and at the timing of writing ongoing) review of the Australian *Privacy Act 1998* and also considers the newly enacted *Data Availability and Transparency Act 2022.* The contribution demonstrates that Australia is committed to regulating the disclosure of personal data in a way that balances personal privacy and competing public interests. The review process seeks to modernize Australia's data protection regime and maintain its global interoperability in the digital era. In doing so, Australia's privacy laws are likely to maintain many of their distinctive characteristics that reflect Australia's cultural, economic and legal preferences.

Despite its antipodean location, Australia's legal system appears in many ways quite familiar to European observers. Australia follows the common law tradition,

Normann Witzleb is an Associate Professor at the Chinese University of Hong Kong, faculty of law, and maintains an adjunct position at the Monash University Australia, Melbourne, n.witzleb@cuhk.edu.hk.

Open Access. © 2023 the author(s), published by De Gruyter. BY-NC-ND This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.
https://doi.org/10.1515/9783111010601-009

it is a federal state and a modern liberal democracy. Although Australia's most important trading partners are in Asia and most of its recent migrants also hail from the region, its legal traditions remain still very much aligned with the West. Taking account of its regional connections, Australia has engaged with its Asian neighbors more readily and more extensively in recent decades than in previous times. Australia is a member of Asia-Pacific Economic Cooperation, an inter-governmental forum for 21 economies in the Pacific Rim that seek to promote free trade throughout the Asia-Pacific region. This membership also has importance for privacy protection because the APEC Privacy Framework of 2004 provides an important point of orientation for Australia's privacy regulation. However, as will be further discussed below, the global influence of the EU General Data Protection Regulation (GDPR)[1] can also be felt in Australia's current law reform debates.

B Human Rights Protection of Privacy

Australia has rarely been in the vanguard of protecting privacy interests, but equally it seeks to ensure that it does not stray too far off the mainstream. When describing a country's approach to privacy and data protection, especially to a European audience, it is convenient to start with the applicable human rights framework. The European Union has a rights-based approach to the protection of privacy and data protection, which is evident not least in the separate protection of both these rights in Articles 7 and 8 of the Charter of Fundamental Rights. This double anchoring is, of course, unique to the EU, and a world away from the position in Australia. Australia does not even have a bill of rights or similar human rights catalogue in its federal law. It still follows the traditional position that the common law provides sufficient protection of human rights. There are, however, now an increasing number of states and territories within Australia that do have human rights legislation,[2] although this has so far not had significant effect on privacy protection.[3]

---

1 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 [2016] OJ L119/1.

2 These are the Human Rights Act 2004 (ACT); Human Rights Act 2019 (Qld); Charter of Human Rights and Responsibilities Act 2006 (Vic).

3 Exceptions are cases such as Thompson v Minogue [2021] VSCA 358, in which routine strip searches of prisoners were held to be a breach of the right to privacy in s. 13(1) of the Victorian Charter of Human Rights and Responsibilities Act 2006.

The absence of a federal human rights charter does not mean, of course, that human rights are not protected in Australia. But it does make human rights protection more uncertain and the human rights discourse less explicit. Australia is a party to the International Covenant on Civil and Political Rights (ICCPR),[4] which protects against 'arbitrary or unlawful interference with [...] privacy, family, home or correspondence' in its Art. 17. It has also ratified a range of other UN treaties which protect the right to privacy for specific groups. This includes the Convention on the Rights of the Child[5] and the Convention on the Rights of Persons with Disabilities, both of which guarantee the right to privacy.[6] However, these international human rights protections are not directly applicable in Australian law. They have effect only to the extent to which they are implemented through domestic laws. These laws can be statutes, that is legislative enactments, or the common law, that is the solidified case law contained in decisions of Australian and other common law courts. While the High Court of Australia has held that statutory interpretation must 'favour construction [of legislation] which is in conformity and not in conflict with Australia's international obligations',[7] Australian courts do not acknowledge an overt influence of international human rights obligations on the Australian common law.

C Statutory Protections of Privacy

The most important statute protecting the right to privacy in Australia is the Commonwealth (or federal) Privacy Act 1988. The preamble of the Act makes explicit reference to Australia's obligations under the ICCPR and also declares the Act to be a response to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 (OECD Guidelines).[8] However, the name Privacy Act promises more than the Act in fact delivers. Instead of providing for the comprehensive protection of privacy, the Act merely protects information privacy inter-

4 International Covenant on Civil and Political Rights (1976) 999 UNTS 171.

5 UN Convention on the Rights of the Child (1990) 1577 UNTS 3.

6 UN Convention on the Rights of Persons with Disabilities and its Optional Protocol (2008) 2518 UNTS 283.

7 Minister for Immigration and Ethnic Affairs v Teoh (1995) 183 CLR 273, 287 (Mason CJ and Deane J); Plaintiff M70/2011 v Minister for Immigration and Citizenship (2011) 244 CLR 144, [2011] HCA 32, [247] (Kiefel J).

8 Organization for Economic Co-operation and Development (OECD), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, accompanied by an Explanatory Memorandum (1980).

ests. It would therefore be more accurate to describe it as a data protection statute, rather than a Privacy Act. The Act regulates how Australian Government agencies and certain private sector organizations should handle personal information.

Alongside the federal Act, there are a number of privacy statutes in the Australian states and territories. Like Germany, the Australian states have legislative powers in all areas that are not specifically transferred to, or reserved by, the federal level (called the Commonwealth of Australia, section 51 of the Australian Constitution). The majority of states and territories have their own data protection laws that are specifically directed at state government agencies[9] and, in some cases, also specialized health data laws.[10] Also important are a range of other statutory enactments that protect privacy interests from specific types of invasion, both at Commonwealth and state/territory levels. This includes the federal *Telecommunications (Interception and Access) Act 1979.* In addition, there are state and territory surveillance laws, which regulate the use of surveillance devices – and contain specific regulation for listening devices, optical devices, as well as location and computer tracking.[11]

D Common Law Protection

In line with the UK and other English-speaking countries, Australian law has never seen fit to recognize and protect privacy as a common law right. Part of the explanation for this may be that the concept of privacy is relatively abstract and elusive. It is notoriously difficult to define privacy and to explain its exact scope.[12] It is an umbrella term from which specific protections need to be developed by way of top-down reasoning, that means, from a broad concept to individual applications. This deductive approach is, in some ways, antithetical to the operation of the common

9 Information Privacy Act 2014 (ACT); Information Act 2002 (NT); Information Privacy Act 2009 (Qld); Privacy and Personal Information Protection Act 1998 (NSW); Personal Information Protection Act 2004 (Tas); Privacy and Data Protection Act 2014 (Vic).

10 Health Records and Information Privacy Act 2002 (NSW); Health Records Act 2001 (Vic).

11 Listening Devices Act 1992 (ACT); Surveillance Devices Act 2004 (Cth); 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 1998; Surveillance Devices Act 1998 (WA).

12 See eg, New Zealand Law Commission, *A conceptual approach to privacy* (Miscellaneous Paper, No 19, October 2007) ch 2.

law, which feel most comfortable when it operates from case-to-case, that is using bottom-up or inferential reasoning.[13]

However, despite this challenging starting point, many English-speaking jurisdictions have now improved their privacy protections at general law (ie, common law and equity). Often, it was human rights legislation that prompted an enhanced status of privacy also in private law. This applies most prominently to the United Kingdom, where the enactment of the *Human Rights Act 1998* triggered a revolution of common law rights protections of privacy. The UK initially provided privacy protection through an expansion of the equitable doctrine of breach of confidence.[14] However, the House of Lords soon found that it would be preferable to recognize a separate cause of action in tort law.[15] This new action has become known the tort of misuse of private information.[16] This tort has proven vital in the protection of privacy against the media, in interpersonal relations and many other areas. Other common law countries, such as Canada and New Zealand, have also developed stronger privacy protection through the recognition of specific privacy torts.[17] The courts in these countries were likewise able to take prompts from domestic human rights charters,[18] but were also influenced by the example of US tort law. This is apparent in the fact that they recognized, just as the US, two separate privacy torts – one for the wrongful disclosure of private information another for the wrongful intrusion into seclusion.

These developments, which occurred mostly over the last 20 years, now contrast strongly with the position in Australia. In 2001, the High Court of Australia declared in the decision of *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*,[19] that there was no obstacle to the common law recognizing a

13 See eg, Jeffrey J Rachlinski, 'Bottom-up versus Top-down Lawmaking' (2006) 73 The University of Chicago Law Review 933.

14 Douglas v Hello! Ltd [2000] EWCA Civ 353, [2001] QB 967.

15 Campbell v MGN Ltd [2004] UKHL 22, [2004] AC 457.

16 Douglas v Hello! Ltd (No. 3) [2005] EWCA Civ 595, [2006] QB 125; McKennitt v Ash [2006] EWCA Civ 1714, [2008] QB 73; Vidal-Hall v Google Inc [2015] EWCA Civ 311, [2016] QB 1003.

17 For further discussion, see Jeff Berryman, 'Remedies for Breach of Privacy in Canada' in Jason NE Varuhas and Nicole A Moreham (eds), *Remedies for Breach of Privacy* (Hart Publishing 2018) 323; Chris DL Hunt, 'New Zealand's New Privacy Tort in Comparative Perspective' (2013) 13 Oxford University Commonwealth Law Journal 157.

18 Significantly, neither the Canadian Charter of Rights and Freedoms nor the New Zealand Bill of Rights Act 1990 contain a broad right to respect for private life, as under European human rights law or the International Covenant on Civil and Political Rights (ICCPR). Instead, these instruments provide more limited protection against 'unreasonable search and seizure': Charter of Rights and Freedoms (Can) s 8; Bill of Rights Act 1990 (NZ) s 21.

19 [2001] HCA 63, (2001) 208 CLR 199.

right to privacy but no further steps have since been taken by Australian appellate courts. This position has been confirmed by the High Court as recently as 2020 in *Smethurst v Commissioner of Police.*[20] This puts Australia in a sort of holding pattern, where a privacy tort remains a possibility, but courts have not yet seen a need to recognize it. In the absence of a dedicated privacy tort, privacy interests remain protected only indirectly. Claimants need to rely on a patchwork of causes of action that apply in related areas and protect aspects of privacy incidentally. For example, the tort of defamation can be relied upon where privacy and reputational interests overlap. The tort of trespass to land protects territorial privacy,[21] the equitable doctrine of breach of confidence protects confidential information,[22] and various statutory rules such as copyright[23] and surveillance legislation[24] complete the jigsaw of incidental protection.

The adherence to this conservative position has had the consequence that Australia has over time become an outlier amongst the western common law jurisdictions. The Australian position now shares more commonalities with the law of Singapore,[25] Malaysia[26] and Hong Kong[27] – all of which have likewise not yet taken the step of protecting privacy interests through a dedicated privacy tort.

E The Privacy Act 1988

As mentioned above, the Australian Privacy Act 1988 is the key statute for the handling of personal information. Initially, its scope was limited to Australian federal government agencies. In 2000, it was expanded to cover the private sector,[28] but the Act contains a wide range of exemptions. The most important of these carve outs is the so-called small business exemption which applies to companies with a turn-

20 [2020] HCA 14, (2020) 376 ALR 575.

21 See eg, TCN Channel Nine Pty Ltd v Anning [2002] NSWCA 82, (2002) 54 NSWLR 333.

22 Agha v Devine Real Estate Concord Pty Ltd [2021] NSWCA 29.

23 Copyright Act 1968.

24 See n 11.

25 ANB v ANC [2015] SGCA 43, [2015] 5 SLR 522. See further Singapore Academy of Law's Law Reform Committee, *Civil Liability for Misuse of Private Information* (Report, 2020).

26 Lee Ewe Poh v Dr Lim Teik Man [2011] 4 CLJ 397; See further Usharani Balasingam and Saifullah Qamar Bin Siddique Bhatti, 'Between Lex Lata and Lex Ferenda: An Evaluation of the Extent of the Right to Privacy in Malaysia' (2017) 4 Malayan Law Journal 29.

27 Sim Kon Fah v JBPB & Co [2011] 4 HKLRD 45; See further Yun CJ Mo and AKC Koo, 'A Bolder Step towards Privacy Protection in Hong Kong: A Statutory Cause of Action' (2015) 9 Asian Journal of Comparative Law 345.

28 Privacy Amendment (Private Sector) Act 2000.

over of less than $3 million Australian dollars (which is the equivalent of 2 million €).[29] This exemption, which was introduced to minimize compliance cost for small business operators, has the effect that about 95% of Australian companies do not need to comply with the Act.[30] Other exemptions concern employee records[31] and journalism,[32] as well as registered political parties[33] and political acts and practices.[34] These exemptions significantly reduce the scope of application of the Privacy Act. However, the justifications of these exemptions have increasingly been put into question[35] – not least because comparable countries do not make use of similar carve outs. For example, the political exemption, which has the effect that Australia's political parties as well other political actors do not need to comply with privacy principles, was initially justified with the consideration that it would help with implied freedom of political communication. However, in more recent times it has become apparent that unrestricted data practices of political actors can themselves pose danger to political discourse and democratic decision-making.[36] A particularly problematic aspect of the exemptions is that these actors cannot be held legally accountable for their data processing practices, and that Australian citizens have very little insight into what happens with personal data in the political process.[37]

Following a comprehensive review of Australian privacy laws in 2008 by the Australian Law Reform Commission,[38] the Privacy Act was amended in 2012.[39] Among the important changes was the amalgamation of two previously distinct sets of privacy principles that applied to the public and private sectors, respectively. Now, a single set of so-called Australian Privacy Principles (APPs) applies in

29 Privacy Act 1988 ss 6C, 6D.

30 Australian Government, Office of the Australian Information Commissioner, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner* (2020) [4.11].

31 Privacy Act 1988 s 7B(3).

32 Privacy Act 1988 s 7B(4).

33 Privacy Act 1988 s 6C.

34 Privacy Act 1988 s 7C.

35 Australian Government, Attorney-General's Department, *Review of the Privacy Act – Discussion Paper* (2021) chs 4–7.

36 Information Commissioner's Office (UK), *Democracy disrupted? Personal information and political influence* (2018).

37 Normann Witzleb and Moira Paterson, 'Voter privacy in an era of big data: Time to abolish the political exemption in the Australian Privacy Act' in Normann Witzleb, Moira Paterson and Janice Richardson (eds), *Big Data, Political Campaigning and the Law: Privacy and Democracy in the Age of Micro-Targeting* (Routledge 2020) 164.

38 Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice (ALRC Report 108, 2008).

39 Privacy Amendment (Enhancing Privacy Protection) Act 2012.

largely identical form to all entities covered by the Privacy Act.[40] These APPs govern the collection, use, disclosure and storage of personal and sensitive information and how individuals may access and correct records containing such information. The principles differ from those in the GDPR in several key respects, as will be explained below. Similar to the GDPR and other data protection laws, the Privacy Act only applies to 'personal information'.[41] The current definition of 'personal information' was inserted into the Privacy Act in 2012. The definition states: information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.

There has been some controversy around the word 'about' in this definition, which differs from 'relating to' in the GDPR. In a 2017 decision, the Full Court of the Federal Court confirmed a tribunal decision which had held that 'about' means that the information needs to have some biographical relevance for the individual concerned.[42] This has raised doubt as to whether the definition also applies to more technical information, such as device identifiers, IP addresses or location data.[43] Such information is potentially linked to an individual, but only has a tenuous connection to a person's life.

Australia also provides stricter protections for certain categories of information that are regarded as particularly sensitive. This might be seen as slightly surprising given that Australia, as other common law countries, based its data protection laws on the OECD Guidelines, which recognize the issue of sensitive data without, however, adopting that concept.[44] In a similar vein, the APEC Privacy Framework also does not single out specific categories of personal data as having a 'sensitive' quality and as such meriting extra legal protection.[45] Yet, in the Australian context, the appeal of the predominantly European idea of giving certain categories of data more protection has won the day. It seems ultimately to have outweighed concerns about the potential divergence with other common law regimes in the region, such as Canada and New Zealand, which do not recognize the 'sen-

40 Privacy Act 1988 Sch 1.

41 Privacy Act 1988 s 6.

42 Privacy Commissioner v Telstra Corporation Ltd [2017] FCAFC 4, (2017) 249 FCR 24.

43 Joshua Yuvaraj, 'How About Me? The Scope of Personal Information under the Australian Privacy Act 1988' (2018) 34 Computer Law and Security Review 47; Julian Wagner and Normann Witzleb, 'Personal Information' in the Australian Privacy Act and the Classification of IP Addresses' (2017) 3 European Data Protection Law Review 528.

44 Ibid, [1].

45 Asia-Pacific Economic Cooperation (APEC), Privacy Framework (2015).

sitive information' categories but adopt a more contextual approach.[46] The Privacy Act largely mirrors the EU's special data categories, although the additional protections available to such data are more restricted than under the GDPR.

F The Review of the Privacy Act

For the last two years, Australia has been engaged in another review of its Privacy Act.[47] The fact that Australia's privacy rules have not been subject to major review and reform for more than a decade is beginning to show because technology and commercial practices have developed significantly since then. A central objective of the reforms is to respond to the rise of digital platforms, big data analytics, and the increasing reliance on AI. There is growing recognition that the current Australian rules do not sufficiently protect digital privacy in a data-driven world and that they are increasingly falling short of community expectations.[48] Concerns arise in several areas, including in relation to the definition of personal information, the notice and consent requirements, the protection of children's personal data, and the strength of enforcement rights. Each of these will be discussed below, but space does not permit consideration of the protection against inferences, the use of automated decision-making, the right of erasure and other issues.

One of the triggers for the review was the recommendations to reform privacy laws made by the Australian Competition and Consumer Commission (ACCC). The ACCC, which is the regulator of market conduct, engaged in a very comprehensive and influential review of Digital Platforms from 2017–2019.[49] The ACCC Inquiry examined the transformative impact of digital platforms on the news media and advertising sector. Data protection and privacy laws were just one aspect of a broad-ranging inquiry that also included competition law, media law and consumer protection law.

---

46 Damian Clifford, Megan Richardson and Normann Witzleb, 'Artificial intelligence and sensitive inferences: new challenges for data protection laws' in Mark Findlay and others (eds), *Regulatory Insights on Artificial Intelligence: Research for Policy* (Edward Elgar, 2022) 19.

47 Attorney-General's Department, *Privacy Act Review: Issues Paper* (October 2020) and Attorney-General's Department (n 35). At the time of writing the Attorney-General's Department's Final Report was completed but yet unpublished.

48 Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2020* (2020).

49 Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, 2019).

One recommendation in the Final Report of the Inquiry that made international headlines was the suggestion for a news media bargaining code, which obliged the very large digital platforms that operate in Australia to pay local news publishers for the news content they made available through links on their platforms. This recommendation was accepted by the Government but strongly resisted by social media platforms, which feared that mandatory payments to news organizations might provide a model for similar laws in other countries. The code has eventually gone ahead, although it was somewhat watered down, and gives news publishers, including some public interest publishers, now some extra income which is taken from the profits made by the likes of Facebook and Google. This code is noteworthy for two reasons. The first is that it is one of the relatively rare examples where an Australian Government was prepared to take an internationally leading role in digital information regulation. The second reason is to show that, when the Australian Government chooses its battles wisely, it can succeed with its regulatory aims, even against the largest multinational corporations. Australia, although economically a smaller jurisdiction, is not condemned to be a follower.[50]

A second important reform process in recent times included the Australian Human Rights Commission's inquiry into Human Rights and Technology.[51] The remit of this inquiry also went beyond data protection, because it examined the impact of new technologies such as AI across the field of human rights. The Commission made proposals for responsible AI regulation, including addressing the use of biometric information and surveillance technologies. In particular, the Report recommended proactive protections of human rights in the development and use of these technologies, including the introduction of a right to privacy and a moratorium on the use of biometric technologies in high-risk decision making until proper regulation is in place.

These two reports have confirmed that Australia's privacy laws need to be reformed to respond appropriately to new technologies. The GDPR is widely regarded as the gold standard for data protection in many parts of the world,[52] going much beyond Europe itself. The 'Brussels effect' on the data practices of multinational

50 Another example is the 'plain-packaging laws', which required all tobacco products to be sold in standardized packaging that does not allow for any logos or promotional texts: Suzanne Zhou and Melanie Wakefield, 'A Global Public Health Victory for Tobacco Plain-Packaging Laws in Australia' (2019) 179 JAMA International Medicine 137.

51 Australian Human Rights Commission, *Human Rights and Technology* (Final Report, 2021).

52 See eg, Alessandro Mantelero, 'The future of data protection: Gold standard vs. global standard' (2021) 40 Computer Law & Security Review 105500, https://doi.org/10.1016/j.clsr.2020.105500. Critical: Lothar Determann, 'California Privacy Law Vectors for Data Disclosures', in this volume, at 121, 141 et seqq.

corporations has been well documented.[53] For these companies, it makes economic sense to adopt a single set of rules – and often they prefer to follow the rules set in Brussels for all their operations worldwide, rather than differing rules in different markets.[54] But apart from setting *de facto* standards for data processors, the GDPR also influences law-making in some countries. Some countries choose to align themselves closely with EU data protection framework because they desire to achieve adequacy status under the EU rules. However, that is a significant driver only for a relatively small number of countries.[55]

Unlike its regional neighbors New Zealand, South Korea or Japan, Australia has never applied for an adequacy decision. The wide exemptions in the Privacy Act have previously been identified as the main obstacle to obtaining an EU adequacy decision.[56] But even for countries that do not seek alignment with EU rules, the GDPR provides a benchmark for comparison. Throughout the recent Australian debate on updating the privacy framework, the GDPR has remained a constant reference point in the discussion. In other words, the 'Brussels effect' can be felt in Australia, too. However, even Australia's privacy regulator, the Office of the Australian Information Commissioner (OAIC) is not explicitly advocating for reforms that would guarantee to achieve adequacy under EU rules. Instead, it considers 'interoperability' of the Act with overseas privacy regimes overseas, including the GDPR, to be the more important objective and is content to leave the decision on whether to seek adequacy in the hands of the Australian Government.[57]

G Key Aspects of the Proposed Privacy Reforms

This section will consider and evaluate some of the key issues addressed in the reform. However, given that the Final Report of the current inquiry is still unpublish-

53 See generally Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (New York: Oxford University Press, 2020).

54 Lee A Bygrave, 'The "Strasbourg Effect" on data protection in light of the "Brussels Effect": Logic, mechanics and prospects' (2021) 40 Computer Law & Security Review 105460, https://doi.org/10.1016/j.clsr.2020.105460.

55 The EU has so far recognized Andorra, Argentina, Canada (in relation to commercial organizations), Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, the United Kingdom under the GDPR and the Law Enforcement Directive, and Uruguay as providing adequate protection.

56 Article 29 Data Protection Working Party, Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000.

57 See discussion in Office of the Australian Information Commissioner (n 30) [8.35]–[8.40].

ed at the time of writing, the Government has yet to reveal its preferred approach on many issues and comments on the likely future shape of the laws are necessarily preliminary. Nonetheless, it is worthwhile to provide an overview of some of the identified issues and the degree to which Australia engages with international approaches on these matters.

I Definition of Personal Information

As mentioned above, the Australian definition of personal information is seen as slightly narrow at present. The proposals are to broaden the definition along the lines of the GDPR and, in line with international models, to replace the word 'about' with 'relating to'. This would clarify that non-biographical information relating to a person is included in the definition. It is also likely that the revised definition will clarify that 'inferred information' can be personal information. There is also significant stakeholder support to make individuation, rather than identifiability, of a person the touchstone of protection.[58] This is because many modern forms of profiling, such as behavioral advertising, do now operate without knowledge of a person's identity. These processes are based on a person's attributes (such as their income, marital status, residential suburb), rather than their identity, and draw inferences from these attributes to arrive at their interests, preferences and susceptibility to certain messages. A person may therefore suffer privacy harm in the form of loss of autonomy, manipulation, unwelcome targeting or discrimination, even if their identity is unknown throughout the process. While the GDPR also still links personal data to identification or identifiability,[59] it is arguably more alert to the digital harms that can arise when a person is 'singled out' on the basis of their personal characteristics.[60] More recent regimes such as that of California are moving beyond that,[61] because they also capture information that can be associated with a particular individual, whether they are identifiable or not. It is therefore to be welcomed that the Discussion Paper for the Privacy Act Review proposes that the updated definition would cover 'circumstances in

58 See Attorney-General's Department (n 35) 22–23; see further Anna Johnston, 'Individuation: re-imagining data privacy laws to protect against digital harms' (2020) Brussels Privacy Hub, Working Paper No 6.24 <https://brusselsprivacyhub.eu/publications/wp624.html> accessed 07.02.2023.

59 GDPR (n 1) Art. 4.

60 See eg ibid rec 26.

61 Californian Consumer Privacy Act 2018, s 1798.140(o)(1): 'Personal information' means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.'.

which an individual is distinguished from others or has a profile associated with a pseudonym or identifier, despite not being named'.[62]

II Strengthening Notice and Consent

In its present form, the Privacy Act gives significant room to data processors to seek consent through bundled, opaque and implicit processes that manipulate or undermine consumer choice. Many consumers do not read privacy notices and, if they read them, do not understand them. The Digital Platforms Inquiry suggested a range of measures to strengthen notice and consent, such as multi-layered and standardized notice and consent processes, as well as pro-consumer defaults.[63] These were intended to make the giving and withholding of consent easier and to ensure that the consumers are better informed when making their privacy choices. However, critics argue correctly that there are fundamental problems with the notice-and-consent model.[64] This is because of the well-established concerns that consumers are at a structural disadvantage when confronted with the myriad of privacy notices, including 'cognitive bias, bounded rationality and limits in time and experience in reading terms with legal import'.[65] Moreover, even if notices were read and understood, voluntary consent is in many cases illusory because data subjects are often not free to choose: if they want to access a particular service or are in a relationship of dependency, they need to accept the terms and conditions even if the proposed data practices contradict their preferences.[66] The GDPR does better in this area, including by having stricter notice and consent requirements. For example, it requires that employers generally need to find a basis for data collection and processing other than consent since employment causes

62 Attorney-General's Department (n 35) 27.

63 Australian Competition and Consumer Commission (n 49) rec 16.

64 See eg Damian Clifford and Jeannie Paterson, 'Consumer Privacy and Consent: Reform in the Light of Contract and Consumer Protection Law' (2020) 94 Australian Law Journal 741; for a comparative perspective, see Leon Trakman, Robert Walters and Bruno Zeller, 'Digital consent and data protection law – Europe and Asia-Pacific experience' (2020) 29 Information & Communications Technology Law 218.

65 Clifford and Paterson (ibid) 747.

66 The APP Guidelines state that consent will be voluntary if an individual 'is given a genuine opportunity to provide or withhold consent': Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines [B.43]. The requirements of consent, such as its voluntariness and whether it can be implied have been interpreted more strictly in recent determinations: Flight Centre Travel Group (Privacy) [2020] AICmr 57; Commissioner initiated investigation into Clearview AI, Inc. (Privacy) [2021] AICmr 54.

power imbalances that stand in the way of providing 'free' consent.[67] It is likely that the Australian reforms will reduce the scope for notice-and-consent as a justification for data collection and processing, and adopt more restrictions or even outright bans on some practices that are likely to cause harm to consumer interests.[68] During the consultations, it became apparent that there is also significant support for a general requirement to handle personal information in a fair and reasonable manner,[69] which already exists in the data protection laws of New Zealand[70] and Canada.[71] At this stage, it remains an open question whether the Government will press ahead with its intention to impose stricter requirements on social media platforms, which it proposed should be embedded in a binding Digital Platforms Privacy Code.

III Better Protection of Children's Privacy

Another area in which international developments are highly influential in the Australian debate are the data rights of children. The *Privacy Act 1988* currently contains no specific provisions regulating the privacy of children or young people and offers no additional protections to them.

As a result, where data processing requires consent, the ordinary principles relating to consent, and the capacity to give consent, apply.[72] If a child provides consent, this consent is valid only if the child has the requisite capacity to consent to the data processing in question. Capacity requires that the child has sufficient understanding and maturity to understand what is being proposed.[73] Currently, the OAIC's Australian Privacy Principles Guidelines suggest that, if it is not practicable or reasonable for an APP entity to assess a child's capacity on a case-by-case basis, the entity may rely on two presumptions: first, that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise; and

67 European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 (2018) [21]–[22].

68 The Government has also proposed a binding Digital Platforms Privacy Code that would impose stricter requirements on social media platforms.

69 Attorney-General's Department (n 35) 85.

70 Privacy Act 2020 (NZ) s 22 (Information Privacy Principles 4 (b) (i), 10 (1) (d) and 11 (10 (d)).

71 Under Personal Information Protection and Electronic Documents Act 2000 (Can) s 3, an organization 'may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances'.

72 In Victoria, Privacy and Data Protection Act 2014 (Vic) s 28 contains detailed provisions on capacity to consent and the giving of consent by a representative.

73 APP Guidelines (n 66) B52.

second, that a child under 15 does not have capacity to consent.[74] But there is very little evidence to suggest to what extent these rules are actually observed in practice.

The Government has announced its intention to strengthen the online privacy protections of children and other vulnerable persons,[75] and the ACCC made several specific recommendations to this effect in its 2019 Digital Platforms report. The proposed rules would borrow substantially from the existing regimes in the US, under the Children Online Privacy Protection Rule (COPPA), as well as from the GDPR. A particular influential model is the Age-Appropriate Design Code of the Information Commissioner's Office in the UK (and similar provisions in Ireland) that puts the interests of child users at the center of the design process. Central elements of the Australian proposals are the prohibition of certain harmful practices through so-called 'no-go zones'.[76] This name was first coined in the Canadian context to describe practices that are altogether forbidden or allowed only in limited circumstances,[77] because they are reasonably considered to be inappropriate. In addition, again following the Canadian example, the Australian Government proposals consider introducing an overarching requirement that the collection, use or disclosure of personal data of children must be considered to be in the best interests of the child.[78]

IV A Direct Right of Action

With regard to enforcement, the review is proposing an array of measures to give the OAIC more powers of investigation and sanctioning. In addition, the Government proposes the introduction of a general right of action for interferences with privacy, which would enable direct judicial enforcement action by aggrieved individuals. Currently, the Privacy Act operates primarily as a complaints-based regime.[79] Where a person considers that their personal data has been mishandled, they are generally expected to approach the data processor first and, if no direct

74 Ibid B58.

75 Australian Government, Attorney-General's Department, *Tougher penalties to keep Australians safe online* (Media Release, 2019).

76 Attorney-General's Department (n 35) ch 11.

77 See Office of the Privacy Commissioner of Canada, *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)* (2018).

78 Attorney-General's Department (n 35) ch 13.

79 Privacy Act 1998 s 36.

resolution is reached, they can complain to the Privacy Commissioner.[80] The Privacy Commissioner may investigate into the breach and will dismiss complaints she considers unfounded.[81] If a complaint is substantiated, it is mostly resolved through a non-public conciliation process.[82]

The enforcement powers of the federal Privacy Commissioner,[83] as well as her counterparts in NSW and Vic,[84] include a power to declare that compensation must be paid to a complainant for loss or damage suffered as a result of a privacy interference.[85] Furthermore, tribunals can award compensation in administrative review proceedings.[86]

However, there have been only a small number of determinations[87] and even fewer legal proceedings initiated by the OAIC.[88] In response to the scarcity of its enforcement resources, the 'preferred regulatory approach of the OAIC is to work with entities to facilitate legal and best practice compliance'.[89] Commentators

80 Privacy Act 1998 s 40(1A).

81 Privacy Act 1998 s 41.

82 Australian Privacy Foundation, *Bringing Australia's Privacy Act up to international standards: Submission in response to the Privacy Act Review- Issues Paper* (2020) 33.

83 Privacy Act 1988 s 52; See Normann Witzleb, 'Determinations under the Privacy Act 1988 (Cth) as a Privacy Remedy' in Jason NE Varuhas and Nicole A Moreham (eds), *Remedies for Breach of Privacy* (Hart Publishing 2018) 377.

84 The Privacy and Personal Information Protection Act 1998 (NSW) expressly provides that its provisions do not give rise to any civil cause of action: s 69. However, in administrative review proceedings, the tribunals can award compensation and other relief: Privacy and Personal Information Protection Act 1998 (NSW) s 55 – compensation is capped at AU$40,000: s 55(2)(a). Similar provisions exist under the Privacy and Data Protection Act 2014 (Vic): see s 7 and 78 (compensation cap of AU$100,000, with specific acknowledgment that damages for injury to feelings and humiliation can be awarded).

85 Determinations with compensation awards include: 'EQ' and Great Barrier Reef Marine Authority [2015] AICmr 11; 'D' and Wentworthville Leagues Club [2011] AICmr 9; 'DK' and Telstra Corporation Limited [2014] AICmr 118.

86 The New South Wales Civil and Administrative Appeals Tribunal awarded compensation for breach of the Privacy and Personal Information Protection Act 1998 (NSW) on several occasions, including: CJU v SafeWork NSW [2018] NSWCATAD 300; ALZ v SafeWork (NSW) (No 4) [2017] NSWCATAD 1; and AOZ v Rail Corporation NSW (No 2) [2015] NSWCATAP 179.

87 The determinations are available from the OAIC website <https://www.oaic.gov.au/privacy/privacy-decisions/privacy-determinations> accessed 07.02.2023.

88 The most prominent of the latter is Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4, (2017) 249 FCR 24; but see also Australian Information Commissioner v Facebook Inc (No 2) [2020] FCA 1307 (civil penalty proceedings).

89 Office of the Australian Information Commissioner, 'Privacy regulatory action policy' (2018) [23] <https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy#approach-to-using-privacy-regulatory-powers> accessed 07.02.2023.

point out that giving the courts a greater role in enforcement action would raise the standards of protection and provide greater clarity of statutory requirements in the context of decided cases.[90]

The introduction of a direct right to action for privacy interferences has been recommended by the ACCC in its report on the Digital Platforms Inquiry.[91] After submitter were predominantly in favor of such a right, the ACCC recommended to give individuals and representative classes of individuals the right to seek compensatory damages, including aggravated damages, for the financial and non-financial harm resulting from breaches of the Privacy Act as well as, in exceptional circumstances, exemplary damages.

The various rationales put forward in favor of this recommendation correlate to the perceived weakness of the current enforcement model. The complaints-based enforcement model has long been criticized by stakeholders,[92] because the Australian Privacy Commissioner has had limited enforcement powers and been under-resourced for its multiple functions. In light of the current experience, the ACCC expected that a right of action would not only empower consumers, but also strengthen compliance with the Privacy Act.[93]

The Government has adopted the recommendation for a direct right of action. The Discussion Paper draws mainly on domestic models for the thresholds and modalities that should accompany such a right, such as similar rights under other regulatory regimes. However, submitters also made extensive reference to such rights in other jurisdictions, including the GDPR – generally to argue for a regime that is wider in its coverage and more accessible to individuals.

V A Statutory Privacy Tort

As mentioned above, it is a long-standing issue in Australia whether a privacy tort should be introduced.[94] Law reform bodies have uniformly and for many years an-

90 See submissions to Attorney-General's Department (n 35) 186.

91 Australian Competition and Consumer Commission (n 49) rec 16(e).

92 Australian Privacy Foundation, *Bringing Australia's Privacy Act up to International Standards: Australian Privacy Foundation Submission in Response to the Privacy Act Review: Issues Paper* (2020).

93 Australian Competition and Consumer Commission (n 49) 473.

94 See further Normann Witzleb, 'Another Push for an Australian Privacy Tort: Context, Evaluation and Prospects' (2020) 94 Australian Law Journal 765.

swered this question in the affirmative[95] – but the Government has so far hesitated. A privacy tort is once again on the legislative agenda, due to the recommendations by the ACCC as well as the AHRC in the reports mentioned earlier.[96] The ACCC reasoned that a statutory privacy tort would 'lessen the bargaining power imbalance between consumers and entities collecting their personal information, including digital platforms' and provide a deterrent and remedy against 'harmful data practices'.[97] But the proposed tort is not restricted to digital platforms or data misuses and would extend to all types of privacy invasion, including by the media. It would go beyond the Privacy Act, where acts and practices 'in the course of journalism'[98] currently enjoy a broad exemption from compliance with Australian data protection standards.

Unfortunately, the Government Discussion Paper for the Privacy Act Review presented once again only reform options, without expressing a concluded position on whether a statutory cause of action should be introduced.[99] Legislative progress has so far always been hampered by the strong resistance of the media, which (I submit, wrongly) believe that the current uncertain state of the law is preferable over a privacy tort that is the result of careful deliberation and extensive consultation during numerous past inquiries. This is certainly an area where trends in comparative common law jurisdictions point strongly towards reform, yet it remains to be seen whether the overwhelming evidence of strong community support in favor of increased protection is sufficient to overcome government inertia.

95 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report, No 108, 2008); New South Wales Law Reform Commission, *Invasion of Privacy* (Report, No 120, 2009); Victorian Law Reform Commission, *Surveillance in Public Places* (Final Report, No 18, 2010); South Australian Law Reform Institute, *Too Much Information: A Statutory Cause of Action for Invasion of Privacy* (Final Report, No 4, 2016); NSW Legislative Council Standing Committee on Law and Justice, *Remedies for the Serious Invasion of Privacy in New South Wales* (Report, No 57, 2016).

96 Australian Competition and Consumer Commission (n 49) rec 19; Australian Human Rights Commission (n 51) rec 21.

97 Australian Competition and Consumer Commission (n 49) 493.

98 Privacy Act 1998 s 7B(4).

99 Attorney-General's Department (n 35) ch 26.

H The Data Availability and Transparency Act 2022

Another important piece of legislation relevant to data disclosures is the new *Data Availability and Transparency Act 2022*. This legislation was first proposed in the 2017 Report into *Data Availability and Use* by the Australian Productivity Commission.[100] The Act is intended to facilitate better use of public sector data and to encourage innovation, while maintaining trust in the Government's use of public sector data.

The Act creates a new data sharing scheme that allows Commonwealth bodies, so-called 'data custodians',[101] to share public sector data with 'accredited users'.[102] These authorized users are other Australian state and federal government bodies and Australian public universities, but do not include the private sector or foreign entities. Data can only be shared for specified public purposes, namely the delivery of government services, to inform government policies and programs, and for research and development.[103] Enforcement-related purposes are specifically excluded.[104]

Data sharing must be consistent with the Act's data sharing principles[105] and occur pursuant to a registered data sharing agreement.[106] The data sharing principles identify 'project', 'people', 'setting', 'data' and 'output' as relevant parameters for assessing data sharing requests and for managing relevant risks.

Public sector data is defined as data that is lawfully collected, created or held by or on behalf of a Commonwealth body.[107] It includes personal data, although such data can only be shared if additional privacy protections are observed. Several purpose-specific privacy protections restrict the Government's ability to share personal information.[108] In addition, several general privacy protection obligations need to be adhered to.[109] These include that biometric data can only be shared with the consent of the individual. Furthermore, shared data containing

100 Australian Government, Productivity Commission, *Data Availability and Use* (Report, No 82, 2017).
101 See definition in Data Availability and Transparency Act 2022 s 11(2).
102 For details, see Data Availability and Transparency Act 2022 s 11(2).
103 Data Availability and Transparency Act 2022 s 15(1).
104 Data Availability and Transparency Act 2022 s 15(2).
105 Data Availability and Transparency Act 2022 s 16.
106 Data Availability and Transparency Act 2022 Part 2.6.
107 Data Availability and Transparency Act 2022 s 9.
108 Data Availability and Transparency Act 2022 s 16B.
109 Data Availability and Transparency Act 2022 s 16A.

personal information must not be stored, or provided access to, outside Australia. Lastly, if data that has been de-identified is shared, the data sharing agreement must prohibit the recipient from re-identifying the data.

The obligations on data custodians in other legislation, including the *Privacy Act*, need to be considered in the assessment of data sharing requests. However, once data sharing under the *Data Availability and Transparency Act 2022* is permissible and authorized, this authorization also fulfils the relevant authorization requirements for the collection, use and disclosure of personal information under the Australian Privacy Principles.

The Act also establishes the National Data Commissioner and the National Data Advisory Council. The Commissioner oversees the data sharing scheme, including advising on and enforcing it. The Commissioner has the power to make data codes, which data custodians and accredited entities must comply with.

The scheme has the potential to streamline the provision of Government services, which at present is sometimes hampered by the lack of access to relevant data. Whether it achieves its potential for more efficient service delivery will depend on the workability of the Act and the Data Commissioner's template data sharing agreement, as well as the level of trust into the scheme that relevant parties gain. At present, it is not yet clear whether the rules and codes around data sharing will impose the appropriate level of restrictions on custodians and accredited entities in a way that balances measures to curb the potential for misuse or loss of data with the value of the data being shared.

I Lesson from Privacy during the Pandemic

Lastly, it is also important to reflect on Australia's experience with privacy regulation during the pandemic. As is well-known, Australia went its own way during the pandemic adopting a strategy of suppressing the SARS-Co-V-2 virus as far as possible, including through tough border measures.[110] Some parts of the country endured long and strict lockdowns during which public and private life was largely limited to the digital. Australia was also a frontrunner of using electronic means to facilitate contact tracing. It was an early adopter of an electronic tracking app, called COVIDSafe, which relied on proximity tracing. The Government made use of the app voluntary but opted for uploaded data to be stored centrally. In response to community concern over the safe handling of data, the Government created a

110 Anika Stobart and Stephen Duckett, 'Australia's Response to COVID-19' (2022) 17 Health Economics, Policy and Law 95.

stand-alone regime for data collected by the app to maximize download and use of the app.

The COVIDSafe app 'failed'[111] to deliver on its public health objectives because it did not contribute significantly to contact tracing. Nonetheless, it is fair to say that the Australian Government made significant efforts to insulate the data management of the COVIDSafe app from nationwide schemes in the past. Some of these earlier schemes, including the Australia Card and the MyHealth record, suffered from low public confidence and had to be abandoned or were less successful than had been hoped. In contrast, the Government was more attentive to privacy protections in relation to the COVIDSafe app. Positive features included not only the voluntary character of the app, but also measures to prevent indirect coercion to use the app, the limitation of law enforcement access and the inclusion of a right of erasure.

The data protection framework of the European Union was sufficiently developed and flexible to accommodate the unprecedented challenges arising from COVID-19. Australia, however, needed to introduce a standalone legal framework dealing with COVIDSafe contact data because of some evident weaknesses in the existing framework under the Privacy Act.[112] They concern the adequacy of consent requirements, use limitations and the rights to erasure and deletion, data localization rules as well as more broadly the interplay between privacy and other human rights.

However, the lasting legacy of the COVIDSafe app is likely to be that it generated a national conversation around privacy and data practices. Data protection now has greater status in Australia. There is increasing recognition that data protection drives innovation and adoption of modern applications, rather than impedes it.[113] It has become apparent that trust in digital technologies can be undermined when data practices come across as opaque, creepy or unsafe.

The example of the COVIDSafe app shows that robust privacy protections are necessary to achieve a strong uptake of new technologies by the community. There are grounds to assume that Australian society now expects that the Government heeds these lessons more widely, especially in the current review of the general data protection framework contained in the Privacy Act.

---

111 Australian Senate, *Select Committee on COVID-19* (Final Report 2022) [4.113].

112 See further Normann Witzleb and Moira Paterson, 'The Australian COVIDSafe App and Privacy: Lessons for the Future of Australian Privacy Regulation' in Belinda Bennett and Ian Freckelton (eds), *Pandemics, Public Health Emergencies and Government Powers: Perspectives on Australian Law* (The Federation Press 2021) 160.

113 Macmillan Keck, Seharish Gillani and others, 'The role of data protection in the digital economy' (UNCDF Policy Accelerator, 2021).

J Reflections and Conclusion

Australia has an interesting position between the two western trading blocs (Europe and the US) on many issues of data regulation and privacy protection. It is neither aligned with the relative strict approach in the European Union, nor to the more permissive approach in the United States. While Australia has many cultural affinities to Europe, in particular to the United Kingdom, it does not share the human rights culture that underpins data protection regulation in the EU and Europe more widely. At the same time, Australia also does not share the long-held American belief into the superiority and strength of market-based solutions. It has relatively strong general consumer protection laws, but its data protection framework has always trailed behind, both in its substance and its enforcement.

Privacy protection continues to rely on an assemblage of common law and statutory rights, in which new dangers to individual rights are responded to with some delay. Corporate interests in minimizing regulation, be it those of the media or those of small business, have been allowed to influence the shape and strength of the laws. However, there are promising indications that there is now an appetite for stricter regulation. Consumer trust into the data practices of large digital platforms has been steadily eroded, and the pandemic has further reinforced the need for strong protections given society's increasing dependency on data-driven practices.

Australia engages with global trends but usually forges its own path that could be described as middle-of-the-road. The outcome of the current reform process is still unclear, not least because Australia's new federal Government has (at the time of writing) yet to outline its legislative agenda in this field. However, it is likely that the laws will bring evolutionary, rather than dramatic, change and pursue the purpose of making Australia's data protection framework fit for the 2020s. The influence of the European framework is clear, but the GDPR is understood, and referred to, as a benchmark rather than a model. Australia has a long-standing preference for creating laws that are interoperable with international regulatory frameworks, rather than to strive for adequacy with the EU model.

In some ways, the *Data Availability and Transparency Act 2022* is a good example of the direction that Australia likes to take. It is a modern data sharing framework that seeks to create value and efficiencies, that enables innovation and protects trust through granting adequate protections.