EDITORIAL

Information Privacy and Consent in Australia

Information privacy in Australia is commonly traced back to 1969. In a series of Australian Broadcasting Commission (ABC) (now the Australian Broadcasting Corporation) Boyer Lectures, the late Sir Zelman Cowen, an Australian scholar and jurist who later served as the nineteenth Governor-General of Australia, discussed the growing collection of information on citizens by government agencies and their privacy concerns[1]:

> Each of us from the day he's born, begins to deposit information about himself in various public and private files. By the time he emerges from school and the armed forces, the ordinary young adult cannot have escaped becoming the subject of at least a dozen personal information files. Our necessary social interdependence assures an acceleration at the rate at which personal data are accumulated and stored. Until yesterday it's been manila folders; it becomes increasingly a computer record which stores and organizes an ever-wider range of data about each of us. … In face of all the pressures and threats I believe that the claim to privacy is a matter of great and increasing importance in our crowded society, with its unbelievable technological resource and inventiveness. A man without privacy is a man without dignity. The fear that Big Brother is watching and listening, threatens the individual no less than the prison bars.

Later, in 1973, the New South Wales (NSW) Attorney-General, John Madison, commissioned a report into the law of privacy by Professor William Morison of the University of Sydney.[2] Morison approached privacy as an 'interest' rather than as a moral or legal right[3]:

> Privacy may be regarded as the condition of an individual when he is free from interference with his intimate personal interests by others. It is not implied that complete freedom in this respect is anyone's moral right or that he has a legitimate claim that such complete freedom should be his legal right.

As a result of the Morison report recommendations, the NSW Privacy Committee was established under the Privacy Committee Act 1975, as the third permanent data protection body in the world following Sweden and the Land of Hesse in Germany.[4] As noted by Greenleaf, over its nearly twenty-five years of existence, the Committee handled numerous complaints and influenced NSW legislation and government proposals to be less privacy-intrusive.[5] Throughout the 1970s and 1980s several bills to protect privacy were introduced into Australian parliaments, which all failed to be enacted except in NSW.[6]

Since then, as Professor David Lindsay notes, 'Australian privacy law has followed its own path'.[7] The Privacy Act 1988 (Cth) (Privacy Act), the cornerstone of Australia's federal data protection framework, was passed in December 1988 and came into effect in December 2019.[8] The Privacy Act gives effect to the Organisation for Economic Cooperation and Development's (OECD's) 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and observes Australia's obligations under Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[9]

Notes

1 Zelman Cowen, *The Private Man*, The Boyer Lectures, Australian Broadcasting Commission (1969).

2 William Loutit Morison, *Report on the Law of Privacy*, Issue 170 of Parliamentary Paper (Government Press 1973).

3 *Ibid.*, at 3. *See* Greg Tucker, *Frontiers of Information Privacy in Australia*, 3 J.L. & Info. Sci. 63 (1992).

4 Graham Greenleaf, *Privacy in Australia, in Global Privacy Protection: The First Generation* 141 (James B. Rule & Graham Greenleaf eds 2008); *See also* G. K. Gupta, *International Developments in Information Privacy*, 23 Adv. Computers 253, 270 (Marshall C. Yovits ed. 1984).

5 Greenleaf, *supra* n. 4, at 151.

6 *Ibid.*, at 150–151.

7 David Lindsay, *Some Problems of 'Consent' Under Australian Data Privacy Law* 116 (in this issue).

8 Privacy Act 1988, No. 119 (1988 as amended), www.legislation.gov.au/Details/C2014C00076 (accessed 13 Jul. 2022).

9 Office of the High Commissioner for Human Rights, *International Covenant on Civil and Political Rights* (adopted on 16 Dec. 1966), www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (accessed 13 Jul. 2022).

A number of Australian States and Territories have subsequently enacted privacy legislation. In particular, NSW, the Australian Capital Territory, the Northern Territory, Queensland, Tasmania, and Victoria have specific privacy laws governing the processing of personal data by government agencies in those States and Territories.

The Privacy Act regulates information privacy in the Commonwealth public sector and the national private sector, subject to certain exemptions (e.g., businesses with an annual turnover for the previous financial year of AUD 3 million or less, and employee records that are directly related to a past or former employment relationship[10]). The Privacy Act was significantly amended in 2014 and 2017 to enhance the protection of privacy in Australia. Amendments have been made in a number of areas, such as direct marketing, privacy collection statements and privacy policies, collection of unsolicited personal data, disclosure of personal data outside Australia and credit reporting.[11] Significant penalties can now be imposed for 'serious' or 'repeated' interferences with the privacy of data subjects.[12] However, such penalties are comparatively weak when compared to the sanctions available under the EU's General Data Protection Regulation (GDPR).[13]

Similarly, compared to the GDPR, Australia's information privacy laws have not been updated to confer additional rights that have become increasingly important for the protection of privacy in light of new technologies.[14] For example, Australia's information privacy laws do not set out the right to be forgotten, right to data portability, and right to object to the processing of personal information and profiling.[15]

Australia has also enacted far-reaching anti-terrorism and national security laws, including a mandatory retention of all Australians' metadata for two years and access by enforcement agencies without a warrant.[16]

As a result, at a Commonwealth level, Australia's information privacy laws have lagged behind European data protection and privacy developments.[17] Accordingly, unlike New Zealand, Australia's information privacy laws were not declared as ensuring 'an adequate level of data protection' under Article 45 of the GDPR.[18]

Nevertheless, the Australian Government is currently in the process of reviewing the Privacy Act.[19] In October 2020, the Attorney General's Department published an issues paper for consultation,[20] which culminated in the release of a discussion paper in October 2021.[21] This discussion paper highlights the potential for privacy reforms to enhance privacy rights and controls for individuals, including increased controls around notice and consent.[22]

The review takes places alongside the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Online Privacy Bill).[23] Specifically, the Online Privacy Bill will introduce a binding online code for social media and certain online platforms, as well as larger penalties and enforcement measures.[24] However, as of the date of this editorial note, the status of the Online Privacy Bill is uncertain, as it was not introduced in Parliament before the election and has technically lapsed.[25]

Notes

[10] In 2019, the Full Bench of the Fair Work Commission found that the exemption only applies in the case of employee records already held by the employer; *see Jeremy Lee v. Superior Wood Pty Ltd* [2019] FWCFB 2946).

[11] Linklaters, *Data Protected – Australia* (last updated in Jun. 2022), https://www.linklaters.com/en/insights/data-protected/data-protected—australia (accessed 13 Jul. 2022).

[12] *Ibid.*

[13] Under Art. 83(4) GDPR, infringements may be subject to administrative fines up to EUR 20 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

[14] David Watts & Pompeu Casanovas, *Privacy and Data Protection in Australia: A Critical Overview (extended abstract)*, Data Privacy Controls and Vocabularies, Position statements and expressions of interest (2018).

[15] *Ibid.*

[16] Australian Government, *Lawful Access to Telecommunications* (last updated on 17 Mar. 2020), www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-retention-obligations (accessed 13 Jul. 2022); *See also* Rebecca Ananian-Welsh & Keiran Hardy, *Counter-Terrorism Since 9/11: More Laws But Are We Safer?*, The University of Queensland (13 Sep. 2021), law.uq.edu.au/article/2021/09/australian-counter-terror-laws-are-we-safer (accessed 13 Jul. 2022).

[17] Watts & Casanovas, *supra* n. 14, at 3.

[18] *Ibid.*

[19] Australian Government, *Review of the Privacy Act 1988*, www.ag.gov.au/integrity/consultations/review-privacy-act-1988 (accessed 13 Jul. 2022).

[20] Australian Government, *Review of the Privacy Act 1988 (Cth) – Issues Paper* (published on 30 Oct. 2020), www.ag.gov.au/rights-and-protections/publications/review-privacy-act-1988-cth-issues-paper (accessed 13 Jul. 2022).

[21] Australian Government, *Privacy Act Review – Discussion Paper* (opened on 25 Oct. 2021), consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/ (accessed 13 Jul. 2022).

[22] Clarisse Girot, *Australia Status of Consent for Processing Personal Data*, Future of Privacy Forum, 2 (Jun. 2022), fpf.org/wp-content/uploads/2022/06/20220628-ABLI-FPF-Consent-Project-Australia-Jurisdiction-Report.pdf (accessed 13 Jul. 2022).

[23] Australian Government, *supra* n. 16. *See also Online Privacy Bill Exposure Draft (opened on 25 Oct. 2021)*, consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/ (accessed 13 Jul. 2022).

[24] *Ibid.*

[25] Girot, *supra* n. 22, at 3. *See also* Denham Sadler, *Government Fails to Pass 'Landmark' Online Privacy Reforms*, InnovationAus (11 Apr. 2022), www.innovationaus.com/govt-fails-to-pass-landmark-online-privacy-reforms/ (accessed 13 Jul. 2022).

Consent plays a significant role in the Privacy Act. The Australian Privacy Principles (APPs)[26] do not generally require consent for collection of personal information directly from an individual.[27] However, where an entity that is subject to the Privacy Act (APP Entity) collects 'sensitive information',[28] then it must obtain express informed consent from the individual for collection of his/her personal information.[29] This requirement does not apply where the APP Entity relies on an alternative legal basis, such as when collection is permitted or required by law[30] or a 'permitted general situation' or 'permitted health situation'[31] arises. Consent also works as an exception that allows certain processing activities that would otherwise be prohibited under the APPs, such as collection of personal information from a source other than the data subject and cross-border transfers.[32]

The existing consent requirements have been subject to considerable debate during consultation on reform to the Privacy Act, as it is widely recognized that organizations over-rely on consent.[33]

In light of these developments, I am pleased to present this special Australia issue of the Global Privacy Law Review (GPLR), which, in particular, focusses on the role of consent under Australian data privacy law.

I am grateful to Professor David Lindsay of the University of Technology Sydney for sharing his vision in his foreword (*Some Problems of 'Consent' under Australian Data Privacy Law*).[34] He brilliantly summarizes the issues related to consent under Australian data privacy law.

I would also like to thank the authors in this issue, Dr Kayleen Manwaring,[35] Dr Katharine Kemp,[36] and Assoc. Prof. Rob Nicholls[37] for their insightful articles. An earlier version of these articles was published as a report funded by the International Association of Privacy Professionals – Australia/New Zealand Chapter Inc (iappANZ) as part of its legacy grants scheme for research projects advancing professionals in the privacy and data industries.[38] In addition to the general membership of iappANZ, the authors express their gratitude to iappANZ members Katherine Sainty and Melanie Marks, who shepherded them through the grant process, and Professor of Practice Peter Leonard, who acted as proposer. The authors also acknowledge the efforts of their research assistants, Dr Courtenay Atwell, Roseanna Bricknell, Jessica Liu, and Jennifer Westmorland.

Manwaring, Kemp & Nicholls have together compiled a comprehensive analysis of how consent is treated under Australian data privacy law. This work represents a significant contribution to the debate about the future of information privacy under Australian law.

Under the *Report* section, Sophie Dawson & Emma Croft of Bird & Bird discuss the data breach class actions under Australian law.[39] The authors analyse some of the proposed upcoming legislative changes which may have an impact in this regard, such as the proposed introduction of a tort of privacy and direct right of action in respect of interferences with privacy under the Privacy Act.[40]

Under the *Case Note* section, Amy Cooper-Boast & Brooke Hall-Carney of LK Law review the judgment of the UK Supreme Court in *Lloyd v. Google LLC*[41] and analyse how Australia is tackling privacy and data breach litigation.[42] Cooper-Boast & Hall-Carney conclude that while the tide of mass data infringement actions in the UK has, for now, been stymied, class actions are widely available in Australia.[43]

Finally, under the *Book Reviews* section, which is reviewed and edited by our Book Review Editor, Prof.

Notes

[26] Schedule 1 of the Privacy Act.

[27] APP 3.1 and 3.2.

[28] Privacy Act, s. 6(1).

[29] APP 3.3.

[30] APP 3.4(a).

[31] APP 3.4(b) and 3.4(c).

[32] Dominic Paulger & Elizabeth Santhosh, *New Report on Limits of 'Consent' in Australia's Data Protection Law*, Future of Privacy Forum (29 Jun. 2022), https://fpf.org/blog/new-report-on-limits-of-consent-in-australias-data-protection-law/ (accessed 13 Jul. 2022).

[33] *Ibid.*

[34] Lindsay, *supra* n. 7, at 116.

[35] Kayleen Manwaring, *Paradox or Pressure? Consumer Expectations and the Australian Privacy Act* 118 (in this issue), and *'Click Here to (Dis)agree': Australian Law and Practice in Relation to Informed Consent* 127.

[36] Katharine Kemp, *Strengthening Enforcement and Redress Under the Australian Privacy Act* 150 (in this issue).

[37] Rob Nicholls, *Informed Consent to Online Standard Form Agreements* 163 (in this issue), and *Reform in Australia: A Focus on Informed Consent* 177.

[38] Kayleen Manwaring, Katharine Kemp & Rob Nicholls, *(mis)Informed Consent in Australia*, UNSW Law & Justice (Mar. 2021), http://doi.org/10.26190/7sk3-0w49 (accessed 13 Jul. 2022). The views expressed in the report and the articles do not necessarily reflect the views of iappANZ.

[39] Sophie Dawson & Emma Croft, *Missing (in) Action: Where Are the Australian Data Breach Class Actions?* 190 (in this issue).

[40] *Ibid.*

[41] *Lloyd v. Google LLC* [2021] UKSC 50; [2021] 3 WLR 1268.

[42] Amy Cooper-Boast & Brooke Hall-Carney, *Lloyd v. Google LLC, and How Australia is Tackling Privacy and Data Breach Litigation* 195 (in this issue).

[43] *Ibid.*, at 199.

Nikolaus Forgó, we have two brilliant reviews from the University of Vienna.

Iana Kazeeva reviews Prof. Simon Chesterman's *We, the Robots? Regulating Artificial Intelligence and the Limits of the Law.*[44] This book examines how our laws are dealing with artificial intelligence and offers novel observations on its challenges and how they can be addressed. Chesterman impactfully concludes[45]:

> The rule of law is the epitome of anthropocentrism: humans are the primary subject and object of norms that are created, interpreted, and enforced by humans – made manifest in government of the people, by the people, for the people. Though legal constructs such as corporations may have rights and obligations, these in turn are traceable back to human agency in their acts of creation, their daily conduct overseen to varying degrees by human agents. Even international law, which governs relations among states, begins its foundational text with the words 'We the peoples … '. The emergence of fast, autonomous, and opaque AI systems forces us to question this assumption of our own centrality, though it is not yet time to relinquish it.

Theresa Henne reviews Prof. Jan Trzaskowski's *Your Privacy Is Important To U$! – Restoring Human Dignity in Data Driven Marketing.*[46] Trzaskowski explores the application of EU consumer and data protection law to data-driven business models, and suggests how our current legal framework can be informed by psychological, technological and societal perspectives 'to curb predatory business models of surveillance capitalism'. He concludes with a reference to the 'boiling frog' apologue[47]:

> The 'boiling frog'-fable suggests that a frog will be cooked to death if it is placed in water which is heated sufficiently slowly: i.e., we fail to perceive dangers that approach gradually rather than suddenly. Digital transformations that gave us data-driven marketing did appear to come gradually; not slowly but with compelling frames and narratives (storytelling). In reality, frogs change location as a 'natural thermoregulation strategy', … and maybe there are good reasons to gauge the temperature of our own waters – if we can recognise and understand what those waters are.

I hope you enjoy reading this special Australia issue
Ceyhun Necati Pehlivan
Editor-in-Chief

Notes

[44] Iana Kazeeva, *We, the Robots? Regulating Artificial Intelligence and the Limits of the Law by Simon Chesterman, Cambridge University Press, Cambridge 2021. 310 pp. GBP 29.99. ISBN: 978-1-316-51768-0* 200 (in this issue).

[45] *Ibid.*, at 243–246. *See also Conclusion – We, the Robots? Part III – Possibilities* (Cambridge University Press) (published online on 15 Jul. 2021), https://www.cambridge.org/core/books/abs/we-the-robots/we-the-robots/CCFF66EC1711EC214EE6D578E2250077.

[46] Theresa Henne, *Your Privacy Is Important To U$! – Restoring Human Dignity in Data Driven Marketing, Jan Trzaskowski, Ex Tuto Publishing, København 2021. 326 pp. EUR 43. ISBN: 978-87-420-0042-7* 203 (in this issue).

[47] *Ibid.*, at 265.