University of New South Wales Law Research Series

AUSTRALIA DEBATES TOUGHER PRIVACY REGULATION OF DIGITAL PLATFORMS

GRAHAM GREENLEAF

(2019) (161) Privacy Laws & Business International Report, 17-19
[2020] *UNSWLRS* 58

UNSW Law
UNSW Sydney NSW 2052 Australia

Australia debates tougher privacy regulation of digital platforms

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia
[2019] 161 *Privacy Laws & Business International Report*[*] 17-19

Newly re-appointed European Competition Commissioner Margrethe Vestager has signalled that she may introduce broader rules to specifically cover tech companies and their use of data, 'to make sure that the way companies collect and use data doesn't harm the fundamental values of our society,' not just more enforcement of existing rules.[1] Vestager's approach is part of global moves toward tighter regulation of digital platforms,[2] such as Facebook, Google, Amazon and others. The Australian Competition and Consumer Commission (ACCC), and to some extent the Australian government, have taken a prominent early position in these global developments.

The ACCC released the *Final Report* in its *Digital Platforms Inquiry*[3] on 26 July 2019, following a *Preliminary Report* (December 2018). The Australian Government is conducting a public consultation[4] on the ACCC report, and will announce its response and draft legislation before the end of 2019. Although the current global momentum is for multi-faceted regulation involving dissemination of hate speech, abhorrent content, 'fake news', electoral manipulation, copyright breaches and more, this article focuses on the ACCC's data privacy proposals, drawing on a more detailed analysis.[5] The ACCC report addresses some of these issues, and Australia has already established an eSafety Commissioner[6] to address other platform issues, as noted briefly below.

Privacy and markets

With the emergence of the surveillance economy, the collection and use of personal data is the main source of value for digital platforms. The effective control of large data sets exercised by platforms, such as Google and Facebook, creates a power imbalance between platforms and users such that any consent given by users to the collection and use of personal data is illusory. These flows of data have been used to create what is now widely described as 'the surveillance economy',[7] substantially

[*] Valuable comments have been received from Australian Privacy Foundation colleagues, Bruce Arnold, David Lindsay, Roger Clarke, Katherine Lane Nigel Waters and Elizabeth Coombs, but all content remains the responsibility of the author. This article draws on our joint submission to the Australian Government concerning the ACCC Final Report.

[1] F Y Chee 'EU may need to regulate tech giants' data use: EU antitrust chief' Reuters *Technology News* 13 September 2019 <https://www.reuters.com/article/us-eu-antitrust-data-idUSKCN1VY1GU>.

[2] On privacy issues, there are major inquiries into platform regulation in Canada, France, Germany, the European Union, the United Kingdom, the United States and other countries.

[3] ACCC Digital Platforms Inquiry <https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry>.

[4] Joint Media Release (Treasurer; Minister for Communications, Cyber Safety and the Arts) Public consultation on the ACCC Digital Platforms Report now open, 1 August 2019 <http://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/public-consultation-accc-digital-platforms-report-now>. Written submissions were due by 12 September 2019, and invited consultation meetings will take place after that: <https://consult.treasury.gov.au/structural-reform-division/digital-platforms-inquiry/>.

[5] More details are in a joint submission to the Australian government with Australian Privacy Foundation colleagues: Greenleaf G, et al 'Regulation of Digital Platforms as Part of Economy-Wide Reforms to Australia's Failed Privacy Laws (Australian Privacy Foundation Submission to the Australian Government on Implementation of the ACCC's Digital Platforms Inquiry—Final Report)' (September 10, 2019) <https://ssrn.com/abstract=3443337> (hereinafter 'APF Submission on ACCC Report').

[6] eSafety Commissioner website <https://www.esafety.gov.au/>.

[7] The mechanisms of surveillance capitalism are explained in the most comprehensive detail by Shoshana Zuboff *The Age of Surveillance Capitalism* (Public Affairs, NY, 2019), and in her earlier articles. Zuboff argues that surveillance capitalism is a new form of capitalism distinguished by its extraction and exploitation of 'behavioural surplus' (personal data collected for the primary

Electronic copy available at: https://ssrn.com/abstract=3502659

invented by Google nearly two decades ago, and shortly thereafter adopted by Facebook. Establishing an effective data privacy regime is therefore essential to correct market shortcomings in the data economy.

The issues at stake go beyond questions of correcting market failures, requiring three broader risks of the surveillance economy to be regulated: (i) its mechanisms compel providers of surveillance services to constantly expand the scope of their collection of behavioural data; (ii) the nature and sources of data used are largely invisible to consumers and citizens; and (iii) the global operation of the largest digital platforms encourages disregard of small scale penalties, resisting effective regulation in most jurisdictions.

In some jurisdictions such as the European Union, these issues have already been addressed to some extent by the GDPR, but this is not so in Australia. The ACCC report attempts to address them.

Fixing Australia's failed privacy laws

Given that Australia has a relatively long history of data privacy laws (state laws from 1975; federal privacy sector in 1988, and private sector in 2001), and a federal Privacy Commissioner since 1988, it is often assumed that its laws are stronger than is the case.[8] Law reform reports recommended wide reforms in 2009, but only a modest strengthening of enforcement aspects was enacted in 2012,[9] plus a rewriting of principles which can be interpreted as a backward step.[10] Since then, enactment of a data breach notification scheme in 2017 is the only positive step.[11]

Into this void, the recommendations of the ACCC, if adopted, present a 'once in a generation' opportunity for serious reform of Australia's moribund privacy laws. Although triggered by the challenges to privacy and other interests presented by digital platforms, their significance in the Australian context is much broader. Each of the main categories of ACCC recommendations, their scope, significance and shortcomings, is now outlined, but without detailed quotation.[12]

Measures to address market power of dominant platforms

ACCC recommends the addition of privacy-related factors in merger laws to include the likelihood that the acquisition would result in the removal from the market of a potential competitor; and the nature and significance of assets acquired, including data and technology. Platforms would be required to give prior notice to ACCC of acquisitions, but this is too weak a recommendation because it only involves a protocol without penalties.

ACCC wants to require choices rather than defaults when operating system providers supply browsers, and when browser providers supply search engines. This recommendation is also too narrow, being limited to the current position with Android browsers, and should be enacted as a general principle, consistent with the principle of Privacy By Design & By Default.

---

purpose of predicting and changing individual behaviours, rather than for the primary purpose of improving a service to individual users). She argues that one of the principal dangers of surveillance capitalism is that its key practitioners are compelled to expand the extent of their surveillance of individuals in order to maintain their dominant positions.

[8] For a history to 2008, see Greenleaf, Graham, 'Privacy in Australia' in Rule J and Greenleaf G (Eds) *Global Privacy Protection: The First Generation*, Edward Elgar, Cheltenham, 2008 <https://ssrn.com/abstract=3072270>

[9] Greenleaf, Graham, 'Privacy Enforcement in Australia is Strengthened: Gaps Remain' (2014) 128 Privacy Laws & Business International Report 1-5 <https://ssrn.com/abstract=2468774>

[10] Waters, Nigel and Greenleaf, Graham, 'Australia's 2012 Privacy Act Revisions: Weaker Principles, More Powers' (2013) 121 Privacy Laws & Business International Report, 12-13 <https://ssrn.com/abstract=2252569>.

[11] Greenleaf, Graham, ''GDPR Creep' for Australian Businesses But Gap in Laws Widens' (2018) 154 Privacy Laws & Business International Report 1, 4-5 < https://ssrn.com/abstract=3226835>

[12] Each ACCC recommendation is set out in full in the APF Submission on ACCC Report.

Electronic copy available at: https://ssrn.com/abstract=3502659

ACCC considered but rejected data portability of personal data, but only did so from a competition perspective, whereas it has already been accepted as a desirable general principle in the EU and elsewhere.

Strengthening Privacy Act protections across the whole economy

Fortunately, ACCC recommends that almost all its privacy-related recommendations apply to all organisations to which the *Privacy Act 1988* applies, not only to digital platforms. The only significant exception is its recommendation for a Privacy Code for Digital Platforms. These economy-wide ACCC recommendations follow, with comments in brackets:

- Update the definition of 'personal information' to ensure that it captures technical data (IP addresses, device identifiers, location data, and any other online identifiers). [This in necessary because Australian case law has excluded IP addresses.]

- Stronger notification requirements so that they apply to all collection, whether direct or via third parties, with few exceptions. Some standard notification elements are recommended, as is use of multi-layered notices and icons. [However they are not detailed enough to ensure data subjects will be aware of the purpose of collection and what will be done with their data.]

- Strong consent requirements: Consent required for collection, use or disclosure, except when required by law, performance of contract, or overriding public interest. 'Valid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent).' Consents cannot be opt-out, implied or bundled. [It is also necessary to restrict secondary uses more tightly than 'related' purposes. 'Take it or leave it' consent requirements also need reform.]

- A right to request erasure of personal information, except when retention is required by law, performance of contract, or overriding public interest. ['Right to be forgotten'.]

- A direct right of individuals to take actions, including class actions, in the courts, to seek compensation for breaches of the Privacy Act. Right to include aggravated and exemplary damages where appropriate. [A similar right has existed in the EU since 1995. In Australia it is essential to avoid data subjects being forced to proceed via complaint to the Privacy Commissioner, a deeply unsatisfactory situation.[13] It has been recommended by many other reviews. A further compensation right, needed to make Australia's mandatory breach notification scheme effective, is for 'statutory damages' to be payable to all victims of such breaches, without need for proof of actual damage by individuals.]

Most of these reforms may seem mundane because they are already included in other countries' laws, but in Australia they are still necessary.

Higher penalties for breach of the *Privacy Act*

ACCC recommends that Privacy Act penalties be increased to equate with *Australian Consumer Law* maximum penalties, namely the highest of A$10 million, or three times the benefit received, or 10% of the (Australian) turnover of the business. The Australian government has already announced its intent to so raise penalties. While equivalence with the 'GDPR standard' for maximum penalties of 2-4% of global turnover might be preferable, the practicability of a medium power like Australia enforcing fines based on global turnover has to be considered.

[13] For reasons, see APF Submission on ACCC Report, 'ACCC R16(e) Introduce direct rights of action for individuals'.

Electronic copy available at: https://ssrn.com/abstract=3502659

Australian Government proposed reforms to the *Privacy Act*

In March 2019, after publication of the ACCC's draft report, the Australian government anticipated some of its proposals, and announced proposed legislation.[14] These seem likely to be merged with its response to the ACCC recommendations at the end of 2019. This proposed legislation, will give more powers and resources to the Office of the Australian Information Commissioner (OAIC) including higher maximum penalties discussed above, and an extra A$25 million over three years.

Both the ACCC recommendations, and the government in its March 2019 legislative proposals, include an enforceable code of practice by digital platforms (DP Privacy Code), covering search, social media, and content aggregation services. It would be developed by the OAIC, with ACCC involved as competition regulator, in consultation with industry stakeholders. It would be enforceable by the OAIC on the same basis as the Act.

From a consumer perspective, further safeguards are necessary: Civil Society organisations must be part of the 'stakeholders' involved; ACCC involvement in enforcement is necessary because of the OAIC's poor track record; and individuals need to be able to go directly to court to enforce the Code, on the same basis as the Act.

ACCC recommends specific content elements of the Code, which mean, in effect, if a controller (an 'APP entity') is designated to be an online platform, a set of higher standards under the *Privacy Act* would apply to it. Some of the ACCC content proposal, depending on implementation, may address core complaints about the business model of surveillance capitalism, and would therefore be serious reforms of international significance, not merely repairs to Australia's sub-standard law. However, they would be improved significantly by addition of other elements found in the GDPR.

Statutory tort for serious invasions of privacy

ACCC recommends introduction of a statutory cause of action for serious invasions of privacy, as recommended by the Australian Law Reform Commission (ALRC), and in similar form by State bodies. This would provides protection for individuals, through the courts, against serious invasions of privacy that may not be captured within the scope of the *Privacy Act*. It is necessary because of the failure of Australia's courts to develop a tort of invasion of privacy, and it would complement the ability of individuals to directly enforce the Privacy Act via the courts. In many instances, court proceedings would be based on both potential actions.

Broader reform of Australian privacy law (ACCC proposals)

ACCC recommends that the government should consider further broad reforms to the Privacy Act, including removal of exemptions '(for example, small businesses, employers, registered political parties)'; requiring fair and lawful processing; 'protections for inferred information'; addressing risks of reidentification; and steps to obtain a positive EU adequacy finding.

Economy-wide consumer law recommendations affecting privacy

ACCC makes two recommendations involving amendments to the *Competition and Consumer Act 2010* which, if adopted, will have a very significant effect on the protection of privacy in relation to digital platforms, and to other categories of businesses adversely affecting privacy. These desirable reforms will also bring consumer protection regulators into central roles in the protection of privacy in Australia, taking the sole responsibility for this out of the hands of the OAIC.

First, unfair contract terms (UCT) would be prohibited (not just voidable), meaning that civil pecuniary penalties (applied by the ACCC) would apply to the use of UCT in any standard form consumer or small business contract, particularly including contracts involving platforms which

[14] Attorney-General, Christian Porter and Minister for Communications and the Arts, Mitch Fifield, Media release: 'Tougher penalties to keep Australians safe online' 24 March 2019 <https://www.attorneygeneral.gov.au/Media/Pages/Tougher-penalties-to-keep-australians-safe-online-19.aspx>.

Electronic copy available at: https://ssrn.com/abstract=3502659

have a zero monetary price. Second, there would be a prohibition on certain unfair trading practices, going beyond the scope of the misleading or deceptive conduct provisions on which Australian consumer law is largely based. This would cover and potentially deter consumer transactions where digital platforms exploit acute information asymmetries and bargaining power imbalances. ACCC says it could cover: inadequate observance of consent requirements; poor security standards; unilateral changes of terms and conditions; overly complex contracts which bury key conditions; and 'all or nothing' click-wrap contracts. These reforms would allow the ACCC (presumably with OAIC input) to pursue systemic problems in ways that OAIC has never achieved.

Recommendations and reforms beyond privacy

Other ACCC recommendations go considerably beyond privacy issues, including: proactive enforcement in markets in which digital platforms operate; an enquiry into ad tech services; designated digital platforms to provide to media authority (ACMA) codes of conduct governing relationships between them and media businesses; mandatory ACMA take-down code to assist copyright enforcement; support for public broadcasters, journalism, and digital media literacy; monitoring 'credibility signalling' by platforms; a Code to counter disinformation; internal dispute resolution requirements for platforms; and an ombudsman scheme to resolve complaints and disputes with platform providers.

Conclusions

The reforms recommended by the ACCC fall into two main categories: first are those which would bring some of the principles and enforcement mechanisms of the *Privacy Act 1988* up to current international standards, the strongest example of which is the EU's GDPR. Second are reforms such as the DP Privacy Code, and the expanded powers under consumer law which are relevant to privacy which go beyond most current data protection laws, and may be useful for consideration in other countries – whether or not they are enacted by the Australian government.

Electronic copy available at: https://ssrn.com/abstract=3502659