Australia's Online Privacy Bill targets social media giants

Graham Greenleaf and Katharine Kemp

[2021] *UNSWLRS* 84
(2021) 174 *Privacy Laws & Business International Report 1*, 5-9

UNSW Law
UNSW Sydney NSW 2052 Australia

Australia's *Online Privacy Bill* targets social media giants

Graham Greenleaf, Professor of Law & Information Systems, UNSW Sydney
& Katharine Kemp, Senior Lecturer in Law, UNSW Sydney

(2021) 174 *Privacy Laws & Business International Report* 1, 5-9

In October 2021, the Australian federal government released draft legislation (the Online Privacy Bill[1]) to amend the *Privacy Act 1988* (Cth) (*Privacy Act*), including both a framework for an 'Online Privacy Code' (OP Code) to impose higher levels of regulation on online platforms, and more general strengthening of the Act's enforcement provisions. It also released a Discussion Paper[2] with 70 proposals – often just 'options' – for a more extensive review of the Act.

The OP Bill and Discussion Paper proposals, when both completed, could become the most extensive proposed changes to the *Privacy Act* since the inclusion of the private sector in 2000. Since 2000, modest changes have been made by re-wording of principles[3] and some enforcement improvements[4] (2014), data breach notification (2018) and COVIDSafe provisions (2020). However, Australia's laws still fall far short of what the GDPR considers 'adequate',[5] and whether the gap will be bridged remains unknown.

Slow-moving reforms

These proposed reforms have been a long time coming. They originate with the Australian Competition and Consumer Commission (ACCC) Final Report in its Digital Platforms Inquiry[6] in July 2019, although the federal government had first floated the idea of a binding code of practice for social media in March 2018 in response to the Facebook/Cambridge Analytica data harvesting scandal. After publication of the ACCC's draft report in March 2019, the federal government had already anticipated some of its proposals and announced proposed legislation directed mainly at stronger enforcement.

After a public consultation on the ACCC's Final Report, the government announced its full response in December 2019, including commitment to legislation for a binding Digital Platforms Privacy Code, to be developed by the Office of the Australian Information Commissioner (OAIC) (but with ACCC involvement), to apply to social media, and to digital

[1] 'Online Privacy Bill Exposure Draft', including *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*, and the Attorney-General's Department *Explanatory Paper*, October 2021 <https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/>

[2] Australian Government *Privacy Act Review – Discussion Paper,* October 2021 <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/ >

[3] Waters, Nigel and Greenleaf, Graham 'Australia's 2012 Privacy Act Revisions: Weaker Principles, More Powers' *Privacy Laws & Business International Report*, Issue 121, February 2013, 12-13.

[4] Greenleaf, Graham 'Privacy Enforcement in Australia is Strengthened: Gaps Remain' (2014) 128 *Privacy Laws & Business International Report* 1-5.

[5] Greenleaf, Graham, 'GDPR Creep' for Australian Businesses But Gap in Laws Widens' (2018) 154 *Privacy Laws & Business International Report* 1, 4-5.

[6] ACCC *Final Report in its Digital Platforms Inquiry* July 2019 <https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry/final-report-executive-summary >

platforms that trade in personal information. This 'Platforms Code' would impose higher standards than otherwise apply under the Privacy Act, and is of international interest.

In relation to broader data privacy issues, the government response was a mixture of acceptance of ACCC proposals with a commitment to legislation, 'support in principle, subject to consultation' on implementation design, and deferral to a further review of the *Privacy Act*, but there were no outright rejections of its recommendations. However, with COVID 19 emerging as a major threat only a month later, visible progress on implementation stalled.

Two years later, the government has in October 2021 announced draft legislation (the Online Privacy Bill[7] – 'OP Bill') which includes both a re-badged 'Online Privacy Code' (OP Code), and the stronger enforcement of the *Privacy Act* that it had long promised. The bottom line is that what was previously promised is being delivered Consultation on this 'exposure draft' was open only until 6 December 2021, and a final Bill will go to Parliament in 2022.

What was previously in the 'support in principle' basket is now a set of *Discussion Paper*[8] proposals for a more comprehensive review of the *Privacy Act*. Submissions to the Attorney-General's Department on the more than 70 proposals are required by 10 January 2022.

Compared with the previous two years of COVID-time, events are moving fast(er), but it is still a complete mess to legislate for half of proposed law reform while still in the midst of consulting about the rest of the package.[9]

The OP Code – new rules for 'platforms' and their friends

At present the Information Commissioner can make only two types of binding Codes: an 'APP Code' specifying how the Act's Information Privacy Principles (APPs) apply to a particular class of entity; and a credit reporting code that sets out additional details of how the Act's credit reporting principles will apply. Now, a third type of binding Code, the OP Code, will specify how designated private sector organisations must comply with both the APPs and with additional obligations.[10]

Like other Codes, industry groups will have first opportunity to propose to draft a code (to be the 'OP Code developer'). If the Commissioner cannot find a suitable OP Code developer, or does not wish to register the Code they develop, then she may develop the Code herself, or modify the industry-developed Code. In either case there will be public consultations.

The OP Code will apply to online organisations (OP organisations) that fall into one of four categories:

1. Social media networks like (the government suggests) Facebook; dating apps like Bumble; online blogging or forum sites like Reddit; some gaming platforms; and online messaging and videoconferencing services like WhatsApp and Zoom. They must be organisations providing an electronic service primarily aimed at enabling interaction

[7] [Exposure Draft] *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*
[8] Australian Government *Privacy Act Review – Discussion Paper,* October 2021 <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/ >
[9] Anna Johnston 'Privacy law reform in Australia – the good, the bad and the ugly' *Salinger Privacy* < https://www.salingerprivacy.com.au/2021/12/03/privacy-act-reform-proposals/>.
[10] The following is based on the Exposure Draft of the Bill, and the Attorney-General's Department *Explanatory paper – Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*, October 2021.

between end-users (disregarding making a profit from advertising), and allowing users to post material on the service.

2. Data brokers whose business model is based on trading in personal information collected online (whether by them or by third parties), for the sole or primary purpose of disclosing the personal information, or information derived from it (such as 'audience' characteristics), including (the government suggests) Quantium, Acxiom, Experian and Nielsen Corporation.

3. Other large online platforms that collect personal information and have over 2.5 million annual users in Australia, like (the government suggests) Amazon, Google and Apple.

4. The Attorney-General can also apply the OP Code, by legislative instrument, to other classes of organisations, where satisfied (only) that this is in the public interest, and the Information Commissioner has been consulted (s. 6W(7)). Such flexibility should make it more difficult for organisations to avoid the application of the OP Code. Any such legislative instrument will be subject to Parliamentary review and disallowance processes.

There can only be one OP Code (see note to new s. 26KA), even though there are a wide variety of organisations to which it will apply. The only way this will make sense is if part of the Code is generic, and other parts apply to only some of the four categories of OP organisations.

The OP Code will impose higher standards for OP organisations than otherwise apply under the *Privacy Act*. The main requirements the Code will impose follow:

- Content of privacy policies and notice to individuals will go beyond the current APP requirements.

- Higher standards for what qualifies as 'consent' will apply, intended to require that it is 'voluntary, informed, unambiguous, specific and current'. The draft legislation will require some amendment to achieve this. This draws on the GDPR's definition of consent. Where 'sensitive' information is involved, OP organisations will need to seek renewed consent periodically, or when circumstances change. The 'specific' consent requirement may rule out unrelated uses such as market research.

- OP organisations will have an obligation to comply with a consumers' reasonable request that the organisation stop using and disclosing their personal data. For example, Amazon currently states in its privacy policy that it uses its customers' personal data in its advertising businesses and that it discloses customers' personal data to its vast Amazon.com corporate group. It would have to stop this, at a customer's request. The Bill allows companies to charge a 'non-excessive' fee for compliance. Secondary uses currently allowed under the Act will continue to be allowed. This is a very weak version of the EU's 'right to be forgotten', and a weaker version of the erasure right recommended by the ACCC.

- Details of how existing privacy protections (ie the APPs) apply to children and other vulnerable groups will now be set out in the Code, rather than in guidance materials from the Commissioner. This will include how consent should be obtained.

- For social media services, like Facebook and WhatsApp, there will be stronger requirements than for other OP organisations, including:

- To take reasonable steps to verify the age of social media users;
- To obtain parental consent before collecting, using or disclosing personal information of a child under 16, including taking reasonable steps to obtain such consent if the service later becomes aware that a child is under 16; and
- To ensure that data practices are 'fair and reasonable in the circumstances', with the best interests of the child as the primary consideration in determining this. The Code may define what is 'fair and reasonable'.

The Discussion Paper proposes that some of these requirements will be imposed more generally on all data controllers, once the whole Act is reviewed. There are other optional topics which the Commissioner or OP Code developer may choose to include, including imposition of additional requirements not found in the APPs, and obligations to report complaints received by the Commissioner.

The Commissioner's full range of investigatory and enforcement powers can be used to enforce the Code. For both Commissioner-developed and industry-developed OP Codes, the Commissioner must consult and have regard to the views of both the ACCC and the eSafety Commissioner, before deciding whether to register an OP Code.

Will it make any difference?

What are the main weaknesses in the OP Code proposals? There are unfortunately plenty of opportunities for the large platforms to delay these rules from taking effect. Companies could waste many months claiming they wish to be the OP Code developer but prove unwilling to propose effective regulation. More months could then be wasted in consultations pointing out the weaknesses in what is proposed. Companies are also likely to use opportunities to challenge the content of the Code, and their inclusion in its coverage. A key tactic companies will likely use to evade these rules is to claim that their business is not using personal information when they hold onto personal data and use it for new purposes. This is because the OP Code and the *Privacy Act* only apply to 'personal information', as defined in the Act, which will not be broadened until the whole Act is reviewed. The best reform would be to scrap the proposal for an industry-developed Code, since it is based on the unfounded assumption that the largest practitioners of surveillance capitalism will voluntarily forego data maximisation. Johnston goes further, arguing that since many aspects of the Code are intended to be later implemented in reforms to the whole Act, the whole idea of the Code should be scrapped, and the Act reformed 'for all players, instead of introducing a two-tier regulatory system'.[11]

Some commentators argue that the age verification requirements will result in both identify verification and age verification requirements being imposed on all social media users, resulting in attempted abolition of anonymity in all social media use within Australia.[12] This is part of a broader online media agenda of Australia's conservative government. It will be extremely contentious and might cause the OP Bill to fail.

Stronger enforcement powers – will they be enough?

The Online Privacy Bill will also strengthen the Information Commissioner's (OAIC's) enforcement functions in seven ways, outlined below. The Discussion Paper also contains six proposals relating directly to enforcement by OAIC, and two proposals intended to empower

[11] Johnston, p. 16. – see footnote 9
[12] See for example, Johnston pgs. 14-15.

individuals to protect their privacy via the courts. So we do not yet know which of these Discussion Paper proposals the government will be included in legislation – or when.

The enforcement reforms in the OP Bill cannot be appreciated fully unless the proposed reforms in the Discussion Paper are also considered. For example, items 6 and 12 below are related closely, as are items 1 and 10, and items 2 and 8 (and 9). It would be much more satisfactory if the government had included all aspects of enforcement reform in the OP Bill.

The OP Bill enforcement changes

1. The **maximum civil penalty** for a serious and/or repeated interference with privacy will be increased up to the equivalent penalties in the Australian Consumer Law (ACL). For individuals, the maximum penalty will increase to over $500,000. For corporations, the maximum will be whichever is the greater of $10 million, or three times the value of the benefit received from the breach, or (if this value cannot be determined) 10% of the company's annual *domestic* turnover (with instructions for calculation in the Bill). Unlike the GDPR, this is 10% of domestic, not global turnover.[13] Unfortunately, clarification of the meaning of 'serious' and 'repeated' is to be delayed to the later Discussion Paper reform Bill.

2. The OAIC will be able to issue an **infringement notice** for failing to give information to the Commissioner, when required by the Act as part of an investigation. The penalty will be $2,644 for individuals, $13,320 for companies. Such civil penalty provisions will make it unnecessary for the Commissioner to resort to prosecution of a criminal offence, or to civil litigation. Where such failure constitutes serious or systemic conduct, the Commissioner can seek higher civil penalties before a court or can refer the matter to the DPP for criminal prosecution, and maximum penalties five times as great are possible. [14]

3. To help ensure that conduct found to be in breach is not repeated, OAIC will be given **new powers to make determinations** (decisions) which include a requirement that the respondent engage an independent qualified adviser to advise how they should change their business practices. This has apparently been tested successfully by OAIC.[15] The Commissioner will also be given the power to require respondents to prepare a statement on how their conduct leading to a breach of the Act occurred, and how they have remediated the breach, and to publish the statement or provide a copy to complainants.

4. The OAIC's **powers to conduct assessments** of a company's compliance with the Act, even in the absence of any complaints, will be strengthened by information gathering powers enforceable through the new infringement notice system.

5. The OAIC will have the **ability to share information** with other entities (law enforcement bodies, alternative complaint bodies, and State, Territory or foreign privacy regulators) wherever the Commissioner or the receiving authority is exercising their respective functions and powers, which may include non-privacy functions of the receiving authority and does not require the Commissioner to be transferring a

[13] Explanatory Paper p. 19 refers to 'domestic annual turnover' but the revised s. 13G in the Bill refers to 'relevant turnover', which in s. 13G(4)(e) excludes 'supplies that are not connected with Australia'.
[14] The Explanatory Paper p. 20 is confusing because it does not specify that the higher civil penalty provisions could only be obtained by going to court.
[15] Explanatory Paper, p. 20.

complaint to the receiving body. The Commissioner is given a very wide discretion to transfer information, subject only to being satisfied that the receiving body will protect it. The Commissioner should be required to report how often this power is used.

6. The Commissioner will be **able to disclose information**, on the OAIC website or otherwise,[16] about such matters as determinations or assessments made by the Commissioner, enforceable undertakings, or (with limitations) data breaches, subject to being satisfied that it is in the public interest to do so. When combined with proposal 12 below, these reforms would provide a far higher level of transparency of the Act's operation.

7. The **extraterritorial application** of the Act will be expanded, and thus the scope of OAIC's enforcement powers. The Bill will remove the requirements that, to be liable under the Act, an organisation has to collect personal information in Australia, or hold it in Australia. This will remove the considerable difficulties that exist now in establishing that foreign organisations have collected personal information in Australia, or hold it there. For example, they may collect the information from a digital platform that does not have servers in Australia and is arguably not 'in Australia', or they may obtain the information indirectly from other organisations outside Australia.[17] This expansion of extraterritorial scope should greatly enhance the reach of the OP Code, as well as the Act generally.

Discussion Paper proposals for OAIC enforcement

The Discussion Paper includes proposals to give the OAIC more flexible enforcement options, as set out in 8 – 13 following. The government is not yet committed to legislate on any of these proposals. The Discussion Paper frames these reforms as a possible move from an OAIC 'historically focused on resolving complaints' to one which 'can take more proactive enforcement of privacy standards'.

8. 'A new mid-tier civil **penalty provision for any interference with privacy**, with a lesser maximum penalty than for a serious and repeated interference with privacy' providing an intermediate point between these higher section 13G penalties and the remedies (but not penalties) available under a section 52 determination. At present, penalties apply to only some breaches of the Act. These penalties would require prosecutions. There are no current financial penalty provisions except for serious or repeated interferences with privacy (s. 13G).

9. Another intermediate enforcement mechanism would be 'a series of new low-level and clearly defined breaches of certain APPs with an attached **infringement notice regime**'. For these lesser breaches of the Act, the OAIC could issue an infringement notice, without need for prosecution or civil litigation.

10. There will be **clarifications of what are 'serious' and 'repeated' breaches** under section 13G, and the Court will be given powers to make any orders it sees fit if such

[16] The OP Bill inserts a new s.52(5A) stating that the Commissioner my publish determinations made under s. 52 'on the Commissioner's website', but that is the only limitation on how the Commissioner may make such disclosures.

[17] See examples in Explanatory Paper, pp. 22-23. The OP Bill achieves this in Schedule 2 Part 1 by the deletion of s. 5B(3)(c), the section of the *Privacy Act* that limited the applicability of the Act to where 'the personal information was collected or held by the organisation or operator in Australia or an external Territory…'.

breaches are found. Such clarification would assist controllers and their advisers, the OAIC, the courts, and data subjects and their representatives.

11. The OAIC would be given broader powers to make **declarations requiring mitigation** of actual or foreseeable losses.

12. The OAIC would be required to **increase transparency about the outcomes of complaints** lodged 'including numbers dismissed under each ground of section 41' (where OAIC dismisses a complaint without making a determination under section 52). This will assist somewhat in shedding light on long-standing criticisms that OAIC dismisses complaints which have substance, thereby denying complainants the right of appeal which is only available if a section 52 determination is made. However, to fully address the problem, complainants should be given either the right to require a section 52 determination, or the right to take their complaint directly to a court or tribunal.

13. The OAIC would be given ability to **increase self-funding**, both through industry levies, and through APP entities that are not part of an alternative dispute resolution scheme being required to pay a fee to OAIC as the default complaint handler, if a complaint is made against them.

The proposals for intermediate penalty regimes in points 2, 8, 9 and10, when combined with the much higher penalties in point 1, and the OAIC's enhanced powers to make declarations under section 52 (points 3 and 11), would give the OAIC a far more graduated 'enforcement toolkit', allowing escalation of appropriate enforcement mechanisms. The other element required for a system of responsive regulation[18] is transparency in how enforcement is carried out, and items 6 and 12, if properly applied, will help achieve that. These reforms are all desirable. If the current exemption of 'small businesses' from the Act is removed,[19] then such a tiered system of enforcement will be even more valuable.

What is wrong with this situation is that the OP Bill only includes reforms 1-7, and it is unknown which of proposals 8-13 will be enacted, or when, even though they are inter-related.

Data subjects' direct enforcement rights

Two particularly disappointing elements of the Discussion Paper concerning enforcement involve giving data subjects more direct rights in relation to privacy breaches.

The Discussion Paper proposal to 'create **a direct right of action'** under the *Privacy Act*, so as to give complainants an ability to go 'directly' to the courts for a remedy, rather than through a complaint to the OAIC (with attendant delays and dissatisfaction), is ill-considered. It requires the complainant to first complain to the OAIC, then have the complaint assessed for conciliation, and then obtain leave of the Federal Court or Federal Circuit Court. This is not a 'right' of action, much less a 'direct' one, but a requirement to beg to escape from the system to which the complainant or their representative object. The main purpose of a direct right of action is that it gives those who are already dissatisfied with the OAIC's handling of complaints – as many experienced consumer bodies are – to sidestep the OAIC and take the risk of adverse court costs if they lose. There should be an unconditional right to litigate a *Privacy Act* breach before the courts. If there needs to be a filter to prevent litigation without merit, the courts

[18] Principles of responsive regulation as applied to data privacy are discussed in Greenleaf, Graham *Asian Data Privacy Laws* (OUP, 2014) pgs. 62-73.

[19] The Discussion Paper is equivocal on the removal of this and other exemptions (employee data, political parties and the media). These exemptions are among the main reasons why Australia's law is not 'adequate'.

already have such powers, and the costs of litigation and potential of serious cost orders against the plaintiff will act as a deterrent.

There are many reasons why a direct right of action will be beneficial. There have been only a handful of significant cases on the *Privacy Act* in over 40 years, so no-one yet understands what many of its provisions mean. The means by which the OAIC assesses damages under the Act rests on one successful AAT decision many years ago, and court reconsideration is needed.

There have been no collective actions (class actions or otherwise) by complainants to challenge and creatively disrupt the operation of the *Privacy Act*. In contrast, actions by NGOs (*noyb* and others) under article 80 of the GDPR have been the main driver of the success of the GDPR (the *Schrems* I and II cases, and others). For this to be effective, the Australian 'direct right of action' would have to include a right of complainants to trigger the Court's ability to consider whether conduct complained of constituted a serious or repeated interference with privacy under section 13G, and make penalty orders accordingly.

Another long-running element of Australian privacy debates arises from the failure of Australian courts to develop a **tortious (or equitable) action for breach of privacy**. The best answer is to adopt Option 1 in the Discussion Paper: 'Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123'. The Australian Law Reform Commission's recommendations were for a tort of *serious* invasion of privacy, a conservative and well-considered proposal. The three other options given in the Discussion Paper would be pointless back-pedalling from a reform that has been supported by repeated law reform investigations. Option 3 could usefully be added to Option 1, and would extend the scope of the *Privacy Act*, and of the OAIC's jurisdiction, to deal with 'revenge porn' and similar breaches currently excluded from the *Privacy Act*. It would provide the possibility of actions for redress which do not involve the risk of litigation costs.

What is still missing from the enforcement regime?

All of this strengthening of the Commissioner's investigative and enforcement power is welcome, but it is questionable whether it will in itself make much difference to the overall credibility of the enforcement of the *Privacy Act* while other problems persist.

One significant previous problem, the paucity of OAIC decisions, is already reducing. The number of complaints concerning privacy on which the Commissioner has made final decisions ('s52 determinations') has more than doubled on the average of the last three years (during which the Commissioner received extra funding), compared with the previous three years, from about four to more than 10 per annum. Prior to that the number varied from zero to four per annum. Unless complaints are seen to result in enforceable decisions, all the rest is just window-dressing, and both complainants and respondents (or at least their lawyers) will know that.

Similarly, increasing the maximum civil penalty for a serious and/or repeated interference with privacy to $10 million or more sounds rather more in line with global standards. But the existing section 13G has not resulted in any enforcement decisions after almost a decade.[20] Sanctions are not dissuasive unless they are seen to be used. For this reason, as suggested above, complainants should be able to 'directly' enforce the penalty provisions of the Privacy Act, not only the compensatory provisions.

[20] An action against Facebook related to Cambridge Analytica has not been decided as yet.

In the next issue, the authors will consider the rest of the seventy proposals in the Discussion Paper. Graham Greenleaf is a member of the Board of the NGO Australian Privacy Foundation, and was also an advisory committee member on the Australian Law Reform Commission's reference on a privacy tort. Katharine Kemp is Co-Lead of the 'Data as a Source of Market Power' research stream for the Allens Hub for Technology, Law & Innovation and a Non-Government Advisor to the International Competition Network.