9 December 2021

Australian Government Attorney-General's Department
By email: OnlinePrivacyBill@ag.gov.au.

Submission to Inquiry into Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 and consultation Regulation Impact Statement

About us

The UNSW Allens Hub for Technology, Law and Innovation ('UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

About this Submission

We are grateful for the opportunity to make a submission on the Discussion Paper. Our submission reflects our views as researchers; they are not an institutional position. This submission can be made public.

Our main points relate to:

- The scope of the OP code (how sector is described);
- Alignment of content of the OP code with its scope;
- Additional issues that should be addressed by the OP code;
- General and contextual limits on "reasonable charges"; and
- Empowering the community.

Scope of SM services

It might be worth clarifying in the definition of social media that 'social' includes 'networking' including for professional rather than social purposes.

Alignment of content and scope of OP code

There is always a tension in policy between the kind of generally applicable principles-based regulation in the *Privacy Act* and the particular policy settings that would be more appropriate for a

particular sector.[1] Combining the more general *Privacy Act* with industry-specific codes is one means of resolving the tension. There are, however, risks in a sector-specific approach. For example, media convergence over time will make it likely that what we think of as "social media" will evolve, leading to companies moving in or out of any current definition over time. Because of such challenges, codes should ideally focus *only* on the issues that are specific to the regulated sector, rather than generating unnecessary fragmentation of privacy law.

To the contrary, many of the proposals for the new OP Code could operate instead as amendments to the broader *Privacy Act*. For example, the need for consent to be voluntary, informed, unambiguous, specific and current is not an issue specific to social media or data broking, but should be standard in *all* implementations of APPs 3 and 6 (and is in line with OAIC recommendations more broadly). Ultimately, if the *Privacy Act* reforms include such provisions universally (as is proposed), they may no longer be required in the OP code. But, in any event, using industry codes as a means to strengthen privacy law through a "you first" approach creates fragmentation, with organisations on opposite sides of a scope definitional divide (or the same organisation moving from one side to the other over time) having different requirements for what constitutes "consent". This is not only illogical, it enhances complexity in compliance.

Issues that could be addressed in the OP code

As noted above, the OP code should focus on issues specific to the regulated sectors, rather than attempting a narrow version of general privacy law reform. Below are some suggestions in that regard.

Social media and surveillance

One sector-specific issue that should be dealt with in the new OP code is the question of "who decides" on the limits of government surveillance. Currently, social media companies are enforcing their own rules in this domain, using contract law to prevent those offering access to social media providing access to government agencies with surveillance functions.[2] In particular, companies such as Facebook and Twitter are using terms of service to limit what such agencies can access, even when the information is publicly available. For example, Twitter's developer terms provide "In no event shall your [sic] use, or knowingly display, distribute, or otherwise make Twitter Content, or information derived from Twitter Content, available to any Government End User whose primary function or mission includes conducting surveillance or gathering intelligence." Whatever the policy on government use of publicly available social media content for surveillance purposes ("open source intelligence") ought to be, it is not appropriate that this be dictated by private corporations. The OP code could thus be an opportunity to set parameters in this regard.

[1] Lyria Bennett Moses, 'Sui Generis Rules' in Gary E Marchant, Braden R Allenby and Joseph R Herkert (eds), The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem (Springer Netherlands, 2011) 77 <https://doi.org/10.1007/978-94-007-1356-7_6>

[2] Lyria Bennett Moses, Andre Oboler and Lauren Parnaby, 'Tracking Violent Extremism Oline and the Challenges of Open-Source Intelligence', Global Network on Extremism and Technology (GNET) Insights, https://gnet-research.org/2021/06/02/tracking-violent-extremism-online-and-the-challenge-of-open-source-intelligence/.

Digital "assets"

The New South Wales Law Reform Commission wrote a report on *Access to digital assets and records upon death or incapacity*[3] that, inter alia, deals with the question of who can access digital records after death. This also suggests procedures through which authorised persons can get access to such records. The procedures for this, and how it is managed by social media companies, could be dealt with in the OP code. Note however that these procedures will need to be aligned with the decision at the November 2021 Meeting of Attorneys-General to develop an access scheme for digital records after death or incapacity.[4]

Reasonable charges

If organisations are to be given the power to impose 'reasonable charges' for responding to a request to cease to use or disclose personal data, there should also be (1) a requirement that such charges be waived where applicants can demonstrate that they are not able to bear the costs and (2) a statutory maximum, to avoid overcharging.

Empowering the community

The overarching reason for the government to propose amendments to Australia's data protection regime is 'to better empower consumers, protect their data and best serve the Australian economy'.[5] The government has acknowledged that the need for a binding code of practice for social media and other platforms trading in personal information online is due to a failure of these platforms to ensure that their conduct meets 'community beliefs and expectations'.[6] Additionally, it has recognised that around 70% of consumers consider the social media industry 'untrustworthy'.[7] The current model under the Privacy Act as it applies to these platforms, particularly around notice and consent, has left individuals with a justifiable belief that they lack control over what happens to personal information relating to them, their friends, family and acquaintances.[8] The enforcement role and activities of the OAIC have also come under sharp criticism, due to weak powers under the Privacy Act, severe and sustained underfunding, consequent under-resourcing and lack of regulator skills development.[9] (We do not include in this criticism former or current Commissioners, or other officers of the OAIC, as they have been subject to significant and sustained barriers beyond their realistic control.)

The justifiable lack of trust that individuals and the community have displayed in both the industry and the regulatory response would suggest that individuals and the community should have a far more significant role than currently contemplated in deciding what is acceptable for social media and other platforms to do with their information.

---

[3] NSW Law Reform Commission, *Report 47: Access to digital records upon death or incapacity* (Dec 2019) https://www.lawreform.justice.nsw.gov.au/Documents/Publications/Reports/Report%20147.pdf.

[4] Attorney-General's Department, *Meeting of Attorneys-General (MAG) Communique – November 2021*, (15 Nov 2021) https://www.ag.gov.au/about-us/publications/meeting-attorneys-general-mag-communique-november-2021.

[5] Attorney-General's Department, 'Enhancing online privacy and other measures' *Early Assessment – Regulation Impact Statement* (Oct 2021) https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/, 3.

[6] Ibid.

[7] Ibid 9.

[8] Kayleen Manwaring, Katharine Kemp and Rob Nicholls, *(mis)Informed Consent in Australia* (Report for iappANZ, 31 March 2021) (UNSWorks, http://handle.unsw.edu.au/1959.4/unsworks_75600), ch 1.

[9] Ibid ch 3.

The Code Development process

Despite these legitimate concerns by the community, the OP code development process suggested only contemplates a very minor role for individuals, consumer advocacy groups and the community. A truly worthwhile co-regulatory process should have community, industry and (adequately funded and appropriately resourced) regulators as equal partners.[10]

'First drafter' status for industry grants them a considerable advantage in the process, along with their ability to buy first-class legal and strategic advice. Therefore, we would recommend that even if an industry representative or representatives undertake to develop a code, then representation from individuals and consumer advocacy organisations (such as ACCAN, Consumer Policy Research Centre or Consumer Action Law Centre) should be included as part of the industry development process from the earliest possible time. This consumer representation should be **mandatory**, **funded by industry** (but independent) and **approved** and **monitored** by the OAIC**.** This type of consumer direct involvement in development should happen also if the OAIC takes on the development of the Code, rather than leaving public consultation (which will in its turn likely be dominated by well-funded industry submissions) to an afterthought.

However, this should not replace substantial community consultation once the OP Code is developed: rather, it should be an additional requirement, as the representation will not be able to foresee all community concerns. Additionally, in the Explanatory Paper, consumers appear to have been overlooked in the variation process: they should explicitly be given an equal right with industry to propose variations to the Code for consideration by the OAIC.

New enforcement powers and penalties in the Bill: a direct right of action for consumers?

Most of the new enforcement powers and penalties, greater powers for information sharing and clarification of extraterritorial application set out in the Bill are to be welcomed, subject to our comments above on the **need for alignment of content and scope of the OP code**. We support the appointment of the eSafety Commissioner as an alternative complaint body to allow information sharing. However, as has previously been substantially argued in UNSW Allens Hub research, we would also support a direct right of action for consumers,[11] and considerable increased funding for the OAIC.[12] This would enable both to better meet their existing and new responsibilities under the Privacy Act, including representing the interests of the majority of consumers for whom exercising an individual direct right of action is impracticable.

Yours sincerely,

Lyria Bennett Moses and Kayleen Manwaring

[10] Kayleen Manwaring and Roger Clarke, 'Is your television spying on you? The Internet of Things needs more than self-regulation' (2021) 93 *Computers and Law: Journal for the Australian and New Zealand Societies for Computers and the Law* 31-36, 36.

[11] Kayleen Manwaring, Katharine Kemp and Rob Nicholls, *(mis)Informed Consent in Australia* (Report for iappANZ, 31 March 2021) (UNSWorks, http://handle.unsw.edu.au/1959.4/unsworks_75600) 65-6.

[12] Ibid 66-7.