HERBERT SMITH FREEHILLS

ONLINE PRIVACY CODE: MORE TRANSPARENCY AND MINIMUM STANDARDS FOR DIGITAL PLATFORMS IN AUSTRALIA

15 November 2021 | Insight

G20 nation moves to modernised privacy code for digital platforms, including binding rules. The proposed scope - and stakes for industry players – is substantial.

On 25 October 2021, the Australian Attorney-General's department released, for public consultation, an exposure draft bill introducing amendments to the *Privacy Act 1988* (Cth) (the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth) or **Online Privacy Bill**)[1] and a discussion paper seeking submissions on broader reforms to Australian privacy legislation.[2] Our overview of the Online Privacy Bill and discussion paper is available here.

One of the main amendments proposed by the Online Privacy Bill is the introduction of a framework allowing the Office of the Australian Information Commissioner (**OAIC**) to register an OAIC- or industry-developed, enforceable online privacy code (**OP code**)[3] that would be binding on all large online platforms, social media services and data brokerage services providers (**OP organisations**).[4] This would supplement the current provisions under Part IIIB of the Privacy Act dealing with the development and registration of, and compliance with, APP codes that set out how one or more of the Australian Privacy Principles (**APPs**) will apply to a particular entity or class of entities (and may impose additional requirements).[5]

As detailed further below, large online platforms and social media services are broadly defined in the Online Privacy Bill. This means a wide range of organisations with online operations could be affected by the proposed OP code, going beyond the ACCC's recommendation in its 2019 digital platform inquiry final report to create a privacy code enforceable against social media platforms, search engines and other digital content aggregation platforms.[6]

Along with the removal by the Bill of the condition that a foreign organisation has to collect or hold personal information in Australia to be subject to the Privacy Act, this would also include an organisation that collects personal information of Australians from a digital platform that does not have servers in Australia.

In this briefing, we look at the implications under the Online Privacy Bill for a potential new OP code.

KEY TAKEAWAYS

Submissions on the new Online Privacy Bill close on 6 December 2021. In engaging with the consultation and preparing for the implementation of the OP code, impacted organisations should have regard to the following issues:

- The proposed OP code will prescribe how OP organisations must comply with certain APPs (including the description of uses and disclosures of personal information in privacy policies, as well as notice and consent requirements). It will also impose further requirements on OP organisations to stop using or disclosing information on reasonable requests, and with respect to their interaction with children or other vulnerable individuals.

- Many of the changes that the Online Privacy Bill proposes to introduce through the OP code in respect of OP organisations echo similar reforms contemplated in the context of the discussion paper for the broader economy (eg introducing a right to object, and amending the Privacy Act to expressly provide that consent should be voluntary, informed, current, specific, and unambiguous and privacy notices be clear, current and understandable).

- A breach of the OP code would be treated as an interference with the privacy of an individual, exposing OP organisations to strengthened penalties (of up to the greater of $10 million, 3 times the value of that benefit if determinable or 10% of the relevant yearly turn over) and reinforced enforcement mechanisms otherwise contemplated in the Online Privacy Bill and the discussion paper.

- Particular restrictions regarding the use of the personal information of children align with similar rules under overseas data protection regimes including the EU General Data Protection Regulation (**GDPR**) and reflect a global regulatory focus on the safety of children using social media and the internet generally.[7]

OP ORGANISATIONS

The OP code is proposed to apply to the following types of organisations:[8]

PROVIDERS OF SOCIAL MEDIA SERVICES

DEFINITION

Organisations which provide an electronic service (which are services that allow end-users to access material using a telecommunications 'carriage service' or which deliver material to persons using a carriage service) which:

- have the sole or primary purpose of enabling online social interactions between two or more end-users, including online interaction that enables end-users to share material for social purposes;
- allow end-users to link to, or interact with, some or all of the other end-users; and
- allow end-users to post materials on the service.

EXAMPLES (EXPLANATORY PAPER)

According to the explanatory paper to the Online Privacy Bill (**EP**), this category:

- would cover networking platforms; dating apps; online content services; online blogs or forums; gaming platforms with multiplayer online games with chat functionalities; and online messaging and videoconferencing platforms.
- would not cover services that enable online communications or content sharing as an additional feature, such as online feedback facilities, however neither the Bill nor the EP clarifies that online business interactions will be excluded, unlike under the recently adopted *Online Safety Act 2021* (Cth).[9]

PROVIDERS OF DATA BROKERAGE SERVICES

DEFINITION

Organisations that collect personal information about an individual (directly or indirectly) for the sole or primary purpose of disclosing that information in the course or connection of providing a service.

EXAMPLES (EXPLANATORY PAPER)

The EP explains this is intended to capture organisations whose business model is based on trading personal information collected online, or information derived from such personal information, such as Quantium, Acxiom, Experian and Nielsen Corporation.

LARGE ONLINE PLATFORMS

DEFINITION

Organisations that at a particular time of the year:

- either had 2.5 million end-users in Australia in the previous year, or 2.5 million end-users in Australia in the current year if they did not operate in the previous year; and
- collect personal information about individuals in the course of or connection with providing access to information, goods or services (other than data brokerage services) by the use of an electronic service (as defined above) other than social media services.

EXAMPLES (EXPLANATORY PAPER)

While the EP explains this is intended to capture organisations who collect a high volume of personal information online (such as Apple, Google, Amazon and Spotify), the breadth of this definition has the potential to capture organisations across a wide range of sectors and activities (with most businesses now operating online and using electronic service to provide their goods or services). The Online Privacy Bill expressly excludes customer loyalty schemes and services, which have the sole purpose of processing payments or providing access to a payment system (however this could still capture online banking platforms which offer broader services).

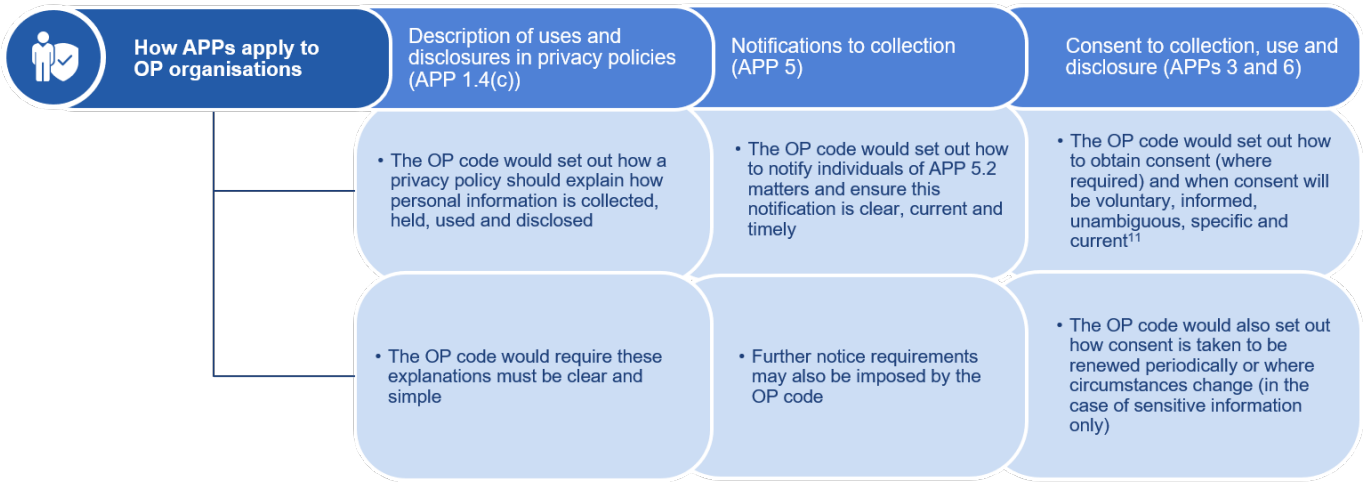
It is currently unclear how inactive accounts or end-users with multiple accounts will be counted to assess whether the 2.5 million end-user threshold is met.

For comparison (albeit in a slightly different context), the EU's proposed Digital Markets Act regulates 'gatekeeper' organisations – essentially organisations with turnover of at least €6.5 billion in the last three financial years (or an average market capitalisation of at least €65 billion), and with 45 million monthly active end users of the core platform service in the EU (roughly 10% of the EU's population) and more than 10,000 yearly active business users in the last three years.[10]

SCOPE OF REQUIREMENTS OF THE OP CODE

EXISTING APP OBLIGATIONS

The Online Privacy Bill provides that the proposed OP code would address how the following APPs apply to OP organisations:



NEW REQUIREMENTS AND RESTRICTIONS

The Online Privacy Bill provides that the proposed OP Code would also impose further requirements and restrictions in respect of:

Ceasing to use or disclose personal information upon request	Interaction with children and other vulnerable users	Optional provisions
Take **reasonable** steps in the circumstances to stop using or disclosing personal information upon individual requests eg in respect of direct marketing, where not impractical.	Stricter rules in relation to children and other persons physically or legally incapable of giving consent. Social media services to: • take all reasonable steps to verify the age of users; • obtain the consent of a parent or guardian of a child under 16 (and take all reasonable steps to verify such consent); and • ensure that the collection, use or disclosure of personal information of a child is fair and reasonable in the circumstances.	The Online Privacy Bill provides that the proposed OP code may also: • specify how any other APPs not set out above are to be complied with by OP organisations (eg the ACCC digital platform inquiry final report recommended this may include provisions regarding information security and retention period requirements under APP 11)[12]; • deal with the internal handling of privacy complaints and provide for reporting of complaints to the OAIC; • require large online platforms to report to the OAIC about the number of end-users they have in Australia; and • be expressed to apply differently to classes of OP organisations, classes of personal information or classes of activities of OP organisations.

DESIGN PROCESS & ENFORCEMENT

ENFORCEMENT

A breach of the OP code would be treated as an interference with the privacy of an individual,[13] exposing covered entities to strengthened penalties (of up to the greater of $10 million, 3 times the value of the benefit derived from the breach if determinable or 10% of the relevant yearly turnover if the benefit is not determinable) and reinforced enforcement mechanisms otherwise contemplated in the Online Privacy Bill and the discussion paper. We will publish a further briefing on those changes shortly.

CODE MAKING PROCESS AND POWERS

The explanatory paper suggests that that industry will lead the initial drafting of the OP Code over 120 days after the Online Privacy Bill receives Royal Assent, with at least 28 days of public consultation. However, the Online Privacy Bill also allows for the OAIC to develop the initial draft in certain circumstances, with a consultation period of at least 40 days.

In deciding whether to register the OP code, the OAIC must consult with at least the Australian Competition and Consumer Commission and eSafety Commissioner.[14] This will allow for each of these regulators to unify their approach in current reform and enforcement action relating to online platforms, having regard to the intersection of privacy, competition and online safety matters in the digital environment.

This article was written by Kaman Tsoi, Marine Giral and Nayan Bhathela

---

1. Online privacy bill exposure draft here
2. Privacy act review discussion paper here
3. As per the proposed new s 26KG in the Online Privacy Bill: Online Privacy Bill sch 1 cl 20.
4. As per the proposed new ss 6W and 26KC(2)(a) in the Online Privacy Bill: Online Privacy Bill sch 1 cl 9, 20.
5. Currently there are two registered APP codes: one developed by the OAIC for Australian government agencies, and one developed by the Association of Market and Social Research Organisations (now the Australian Data and Insights Association) for its members.
6. Digital platforms inquiry final report here, p 481.
7. For example, the recently passed *Online Safety Act 2021* (Cth) contains specific

protections for children against cyber-bullying both inside and outside the social media context. Overseas, the UK's Age Appropriate Design Code also recently came into force, obliging all online apps or services that are likely to be used by children (including social media platforms) to ensure, among other things, that the data of children is not used in a way that detriments their wellbeing and that the data of children is not disclosed unless there is a compelling reason to do so. The UK is also currently debating its own draft Online Safety Bill 2021 which also seeks to impose duties of care on providers of internet services in relation to content that is deemed harmful for children.

8. As per the proposed new ss 6W and 6X in the Online Privacy Bill: Online Privacy Bill sch 1 cl 9.

9. *Online Safety Act 2021* (Cth) subclause 13(2) as clarified by note.

10. EU Digital Markets Act, art 3(2).

11. Australian privacy principles guidelines here

12. Digital platforms inquiry final report here, p 484.

13. As per the proposed new s 13(1A) in the Online Privacy Bill: Online Privacy Bill sch 1 cl 10.

14. As per the proposed new s 26KH in the Online Privacy Bill: Online Privacy Bill sch 1 cl 20.

RELATED TOPICS

Data and privacy

FEATURED INSIGHTS

FEATURED INSIGHTS

HELPING YOU STAY AHEAD OF THE BIG ISSUES

BROWSE BY:

- TECH, DIGITAL & DATA

- GEOPOLITICS AND BUSINESS

- NEW BUSINESS LANDSCAPE

RELATED ARTICLES

UPDATED: UK NATIONAL SECURITY ACT 2021 - WHAT INVESTORS NEED TO KNOW

Foreign investment: Rising tides of politics in regulation

What would a 'reasonable coder' think? Law Commission says no need for new legislation to handle smart legal contracts

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

KAMAN TSOI
SPECIAL COUNSEL, MELBOURNE
+61 3 9288 1336
kaman.tsoi@hsf.com

JULIAN LINCOLN
PARTNER, HEAD OF TMT & DIGITAL AUSTRALIA, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

KWOK TANG
PARTNER, SYDNEY
+61 2 9225 5569
Kwok.Tang@hsf.com

PETER JONES
PARTNER, SYDNEY
+61 2 9225 5588
peter.jones@hsf.com

KATHERINE GREGOR
PARTNER, MELBOURNE
+61 3 9288 1663
Katherine.Gregor@hsf.com

MICHELLE AGGROMITO
SENIOR ASSOCIATE, MELBOURNE
+61 3 9288 1079
michelle.aggromito@hsf.com

MARINE GIRAL
SOLICITOR, MELBOURNE
+61 3 9288 1496
marine.giral@hsf.com