Australian Government

Office of the Australian Information Commissioner

Exposure Draft – Online Safety Bill 2020

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

13 February 2021

OAIC

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the exposure draft of the Online Safety Bill 2020 (the Bill).

2. The OAIC acknowledges the important policy objective of the Bill to keep Australians safe online so that the substantial benefits that come from using the internet can be realised.[1]

3. Most aspects of the daily lives of Australians have been transformed by innovations in technology and service delivery. The scale and scope of technological change – including the emergence of new platforms and services – has given rise to new ways for individuals to interact online and created new risks. Many of these risks have emerged specifically due to the dramatic increase in the amount of data and personal information collected, used, and shared, both in Australia and globally.

4. The OAIC considers that strong data protection and privacy rights are therefore an essential piece in the ring of defence that is being built to address the risks faced by Australians in the online environment. Accordingly, online safety and privacy have distinct but complementary roles to play to achieve the Government's online safety agenda and keep Australians safe online.

5. The Government confirmed its commitment to strengthening and enhancing online privacy protections for consumers in its response to the Australian Competition and Consumer Commission (ACCC)'s Digital Platforms Inquiry (DPI) final report.[2] The DPI final report identified a wide range of potential consumer harms that may arise from the collection, use and disclosure of personal information in the digital environment, including:

   - increased risk of data breaches and cybercrime
   - increased instances of unsolicited targeted advertising
   - third parties leveraging information against the consumer's interest – e.g. price discrimination and psychological profiling which results in manipulation and loss of autonomy
   - discrimination of exclusionary harm as a result of targeting techniques
   - targeted scams, and
   - risks to vulnerable people (including children) of being targeted with inappropriate products or scams, discriminated against or inappropriately excluded from markets.[3]

6. The Government's privacy law reform agenda includes the development of a binding online privacy code with enhanced privacy protections for children and other vulnerable groups, which will apply to digital platforms and other entities that trade in personal information online. The Government is also currently conducting a broad review of the Privacy Act to ensure that

[1] Department of Infrastructure, Transport, Regional Development and Communications (2021), *Online Safety Bill – Reading Guide* (accessed 9 February 2021).

[2] The Treasury (2019), *Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (accessed 9 February 2021).

[3] Australian Competition and Consumer Commission, *Digital Platforms Final Report* (June, 2019).

Australia's privacy framework is proportionate, sustainable and responsive to emerging privacy risks into the future.

Consistency and collaboration

7. The OAIC notes there is the potential for intersection between the proposed online privacy code and measures in the Bill related to the registration of industry codes and the making of industry standards by the eSafety Commissioner. This intersection occurs both in terms of the entities that will be covered and the substantive content of both frameworks which may seek to address issues of common concern, such as consent mechanisms in the online environment.

8. Division 7 of Part 9 of the Bill sets out a framework for the development of industry codes and industry standards for sections of the online industry. 'Sections of the online industry' include social media services, relevant electronic services, providers of designated internet services, internet search engine services and app distribution services (see cl 135).

9. Cl 138 of the Bill sets out examples of matters that may be managed through industry codes and industry standards. The examples include, but are not limited to, 'procedures directed towards the achievement of the objective of ensuring that online accounts are not provided to children without the consent of a parent or responsible adult.'

10. There is some alignment between these definitions and proposed content and the Government's proposed binding online privacy code, which will apply to social media platforms and other online platforms that trade in personal information.[4] The privacy code will require these entities to:

    - be more transparent about data sharing
    - meet best practice consent requirements when collecting, using and disclosing personal information
    - stop using or disclosing personal information on request, and
    - comply with specific rules to protect the personal information of children and vulnerable groups.

11. The OAIC considers that these alignments present an opportunity to address issues of common concern through a coordinated online safety and data protection regime. Ongoing consultation and cooperation between the OAIC and the Office of the eSafety Commissioner will continue to ensure that the distinct but complementary roles of privacy and online safety work effectively and comprehensively to address online risks and harms.

12. The OAIC has significant experience in co-regulatory matters and working with other regulators to avoid unnecessary or inadvertent overlap and to create certainty for consumers and industry. The OAIC has entered into memorandums of understanding with other regulators to achieve

[4] The media release is available at https://www.attorneygeneral.gov.au/media/media-releases/tougher-penalties-keep-australians-safe-online-24-march-2019.

this including the ACCC, the Australian Communications and Media Authority, and the Inspector-General of Intelligence and Security.

13. The OAIC considers that these types of collaborative working arrangements can be most effective where they have a legislative basis to support cooperation and facilitate information sharing.[5] The OAIC recommends that the Bill ensure that the eSafety Commissioner and Information Commissioner have the legislative authority to share information where necessary, to develop a consistent and coordinated approach to the regulation of online safety and privacy.

14. The OAIC also recommends that a provision be included in the Bill to require consultation with the Information Commissioner before the eSafety Commissioner decides to register an industry code or make an industry standard which may intersect with privacy and data protection issues. There is precedent for such consultation requirements in other legislation, for example, s 53 of the *Office of the National Intelligence Act 2018*, s 355-72 of the *Taxation Administration Act 1953* and s 56AD of the *Competition and Consumer Act 2010*.

15. The OAIC has an effective, collaborative and longstanding working relationship with the Office of the eSafety Commissioner and we recommend it is further supported and strengthened through the measures set out in this submission, as we work together to achieve an online environment where safety and privacy is respected and protected.

[5] See section 29 of the *Australian Information Commissioner Act 2010*.