Institute of Public Affairs

IPA RESEARCH NOTE

How the digital duty of care violates the right to privacy

NOVEMBER 2026

Margaret Chambers
Research Fellow

Key findings

By expanding the powers of the eSafety Commissioner under national privacy legislation, the federal government's proposed digital duty of care legislation represents a significant threat to Australians' privacy online:

- The digital duty of care would grant the eSafety Commissioner sweeping powers as an enforcement body under the *Privacy Act 1988*.
- The eSafety Commissioner would have the power to collect "sensitive information" of Australian internet users.
- The eSafety Commissioner and online services would be empowered to share information that identifies individual users.
- The eSafety Commissioner would have the power to share Australians' data with overseas enforcement agencies.
- The eSafety Commissioner would use the information it obtains as fuel for the digital duty of care censorship machine.

These invasive powers will likely have a chilling effect on speech online given the privacy risks associated with a government regulator, eSafety, accessing, sharing, and using personal user information.

Analysis

The digital duty of care would grant the eSafety Commissioner sweeping powers as an enforcement body under the *Privacy Act 1988*

Item 53 of Online Safety Amendment (Digital Duty of Care) Bill 2026 ("the bill"), currently before the Senate,[1] includes an amendment to the *Privacy Act 1988* that would make the eSafety Commissioner an "enforcement body" for the purposes of that act.

Currently, the Commissioner may be considered an enforcement body only "to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law" (s 6(1)(f)). By contrast, if the bill passes, the eSafety Commissioner would be covered in relation to all "enforcement-related activities", which is defined in section 6 of the Privacy Act as including "surveillance, intelligence-gathering, and monitoring activities" as well as breaches of the *Online Safety Act 2021*.

Ordinarily, under the Australian Privacy Principles (APPs), "APP entities", which include both the Office of the eSafety Commissioner and online services, are restricted in various ways in whether and how they collect, use, and share individuals' personal information.[2] However, enforcement bodies are excluded from the APPs in various ways, including for example in permissions to collect personal data without consent, and from obligations to notify users when a privacy leak takes place.

To the extent the explanatory memorandum (EM) addresses the change, it only notes "These powers are necessary to make sure that the Commissioner's enforcement and investigation powers are not inappropriately constrained by provisions of the Privacy Act that would apply if the Commissioner were not an enforcement body for the purpose of that Act."[3] Its commentary mainly focusses on the provisions in the bill concerning children, noting the "collection of personal information is necessary to ensure children are protected from harmful content, activity and service features".[4]

Where the EM comments on the right to privacy for adults, it subordinates it to the overarching legislative goal, providing that "To the extent that obligations in the Bill would require the collection of personal information and limit a user's right to privacy, any such limitation is reasonable, necessary and proportionate to achieving a safe online environment for Australians."[5]

The eSafety Commissioner would have the power to collect "sensitive information" of Australian internet users

Per APP 3.4.(d), enforcement bodies are permitted to collect "sensitive information" about individuals where they "reasonably believe" that the collection is "reasonably necessary for, or directly related to, one or more of the entity's functions or activities".[6]

Under the act (s 6(1)), "sensitive information" includes information about an individual's "racial or ethnic origin", "political opinions", "membership of a political association", "religious beliefs or affiliations", "philosophical beliefs", "membership of a trade union or association", "sexual orientation or practices", "health information", "genetic information" and "biometric data", among other things.

Therefore, under the proposed amendment to the *Privacy Act 1988*, the eSafety Commissioner would be permitted to collect sensitive information without the consent of individuals if doing so is necessary for or related to one of the eSafety Commissioner's functions. These functions are broadly drawn and wide in scope, including promoting online safety and monitoring and enforcing the digital duty of care.[7] This information could be used to profile individual users or identify usage trends across the internet.

The eSafety Commissioner and online services would be empowered to share information that identifies individual users

Per APP 6.2(e), APP entities (online services) are permitted to "use or disclose" personal information, which they would have otherwise been obliged to protect, where they "reasonably believe" that doing so is "reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body" (eSafety).[8]

The eSafety Commissioner and online services would also be permitted to disclose to one another "personal information", which means "information or an opinion" about an individual who is "identified" or "reasonably identifiable".[9] This could include, for example, the individual's name, date of birth, address, online account details, browsing and search histories, recorded interests and preferences, and opinions.

Requiring online services to disclose to eSafety information where it would be "reasonably necessary" as part of its regulatory activities is inherently expansive given the breadth and scope of the digital duty of care's overarching goal to achieve a safe online environment. Given how the framework incentivises over-compliance, the practice of online services complying with requests for information from eSafety could

become an inescapable part of the process affecting Australians who use the internet. In other words, the invasion of user privacy will not be an occasional lapse or "bug" within the system; it will be built into the system itself, raising obvious concerns about surveillance and profiling of individual users.

The eSafety Commissioner would have the power to share Australians' data with overseas enforcement agencies

Under section 212 of the *Online Safety Act 2021*, a function of eSafety is to disclose information to foreign authorities responsible for regulating online safety. This function would be supercharged by eSafety's regulatory responsibility to administer the digital duty of care and its expanded power to collect and use sensitive information.

The Australian Privacy Principles contain rules about the sharing of information. For instance, APP 8.1 provides that APP entities ordinarily must, before disclosing personal information to overseas entities, "take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1)".

Per s 16C of the Act, APP entities are liable for overseas recipients' mishandling of disclosed personal information. However, APP 8.2(f) excludes from those protections an APP entity that is a government agency (like the eSafety Commissioner) where that agency "reasonably believes" that the disclosure is "reasonably necessary" for "enforcement related activities conducted by, or on behalf of, an enforcement body" and the overseas recipient is "a body that performs functions, or exercises powers, that are similar to those [of] an enforcement body". As mentioned, these "enforcement related activities" under the Privacy Act include "the conduct of surveillance activities, intelligence gathering activities or monitoring activities" (s 6(1)), as well as the enforcement of the digital duty of care by eSafety.

The intention here seems to be to facilitate the sharing of personal information for the purposes of law enforcement. But importantly, the obligation on internet services within the digital duty of care captures how they moderate *both* lawful internet use *and* illegal content. In other words, as drafted, the bill will enable eSafety to share the personal user information of law-abiding citizens across borders. It is not constrained by only sharing the user information of criminals.

Users' information is fuel for the digital duty of care censorship machine

The crux of the digital duty of care is to create the mechanism for what the statutory review has described as "an ongoing cycle of risk identification and assessment" and what the EM calls "proactive and ongoing action."[10]

The real heart of the digital duty of care, then, is the risk assessment provisions, which extend beyond the defined statutory harms.[11] Section 27 of the bill requires every online service to undertake written risk assessment identifying "reasonably foreseeable" risks of harm associated with material, conduct, design features, systems and processes, and their potential impacts on persons. In effect, the risk provisions are potentially unlimited in what they consider and affect, and the evident intention is for the process to be as expansive as possible.

The government's recent amendments have removed consideration of user privacy in the risk assessments provisions. It was included in the exposure draft version and subsequently removed when the bill was tabled in parliament.[12]

At the same time, the bill extends the Commissioner's information-gathering powers within the *Online Safety Act 2021*, including criminal penalties for refusing to provide sworn testimony. It also provides that the eSafety Commissioner and "approved researchers:" can operate fake accounts, "sock puppet identities", and operate on online services "for the purposes of performing the Commissioner's functions" and "undertaking

online safety related research".[13] These provisions are broad and ambiguous, including for example the "testing" function permitted in ss 205K(e) and (f), about which the EM does not provide clarity.

Overall, then, the bill dramatically expands eSafety's access to data regarding the operation of online services, user data, and macro trends regarding how users are using services and interacting. These vast information-gathering powers are designed to feed back into the rules establishing and governing the digital duty of care, in particular the regulations and regulatory guidance issued by eSafety which online services will be dependent on to comply with their statutory obligations.

For Australian internet users, then, their online behaviour is monitored, the data is fed back to develop new guidance and rules, and services face strong incentives to adopt them. The digital duty of care would make the violation of Australians' privacy a permanent, structural feature of the internet.

For more information contact Morgan Begg, Director of Research at mbegg@ipa.org.au

End Notes

1. On 28 October 2026, the federal government's *Online Safety Amendment (Digital Duty of Care) Bill 2026* ("the bill") passed the House of Representatives. In the Senate, it has been referred for inquiry, with the government expecting that a final vote to pass the bill into law will take place before Christmas 2026.
2. For the Australian Privacy Principles, see Schedule 1 of the *Privacy Act 1988* (Cth).
3. Online Safety Amendment (Digital Duty of Care) Bill 2026 Explanatory Memorandum, 102.
4. EM, 18.
5. Ibid.
6. *Privacy Act 1988* (Cth), sch 1.
7. *Online Safety Amendment (Digital Duty of Care) Bill 2026* (Cth) sch 2, item 27, proposed s 166B(1) (amending s 27 of the *Online Safety Act 2021* (Cth).
8. *Privacy Act 1988* (Cth), sch 1, cl 6.2(e).
9. Ibid, s 6(1)
10. Above n 3, 70.
11. For a detailed account of the bill, see Andrew Bushnell, *IPA Submission to Online Safety Amendment (Digital Duty of Care) Bill 2026* (Institute of Public Affairs, November 2026).
12. Exposure Draft of the Online Safety Amendment (Digital Duty of Care) Bill 2026, accessible at: https://www.infrastructure.gov.au/department/media/publications/exposure-draft-online-safety-amendment-digital-duty-care-bill-2026.
13. Online Safety Amendment (Digital Duty of Care) Bill 2026 (Cth) Div 3.