Human Technology Institute

22 November 2024

By email: ec.sen@aph.gov.au

Senate Environment and Communications Legislation Committee

Parliament of Australia

Dear Committee Members,

Submission on the Online Safety Amendment (Social Media Minimum Age) Bill 2024

The Human Technology Institute (HTI) welcomes the opportunity to provide a brief submission to the Senate Environment and Communications Legislation Committee (the Committee) on the Online Safety Amendment (Social Media Minimum Age) Bill 2024 (the Bill).

HTI does not, in this submission, express a view on whether there is a compelling public policy justification for the Bill as a whole. We recognise that there are strong, conflicting arguments regarding the policy wisdom, or unwisdom, of the Bill's aim to restrict access to social media for children and young people. In particular, we draw attention to the serious reservations expressed by the Australian Human Rights Commission regarding the Bill, and the Commission's online 'explainer' of a number of the key human rights issues raised by this proposed reform.[1] HTI has itself provided more detailed commentary on implications of age verification technology in two previous submissions, to the Joint Select Committee on Social Media in Australian Society and to the 2024 Statutory Review of the Online Safety Act.[2]

We also observe that this Bill has been introduced in haste, with inadequate time for appropriate consideration of and debate on its content. Such matters clearly merit serious consideration in determining whether the Bill should proceed at all.

Without endorsing the Bill, HTI has drafted this submission on the presumption that Parliament is minded to pass the Bill, but that it is also open to amending the Bill to address a significant flaw in the Bill's protection of the right to privacy. This submission focuses on a loophole in clause 63F(1)(b)(ii) of the Bill, which would enable numerous government entities, and social media companies themselves, to access personal information provided by individuals in the course of age verification, for a broad range of purposes. This provision would serve as a backdoor to increased surveillance of all Australians who access social media sites. As outlined below, the inclusion of this clause would result in a disproportionate interference with Australians' right to privacy under international human rights law, and it is likely to reduce public confidence in the legislative scheme, which would jeopardise its success.

---

[1] 'Proposed social media ban for under 16's in Australia' *Australian Human Rights Commission* (Web Page, November 2024) < https://humanrights.gov.au/about/news/proposed-social-media-ban-under-16s-australia>.

[2] HTI submission to the Joint Select Committee on Social Media in Australian Society (July 2024) HTI submission to the Department of Infrastructure, Transport, Communications and the Arts, Statutory Review of the Online Safety Act 2024 (July 2024).

At a more fundamental level, this provision is completely unnecessary to achieve the Bill's intent – namely, to enact an age restriction on access to social media. On the contrary, it would pursue a completely different policy aim: to enable access for many government and private sector bodies to personal information, including sensitive personal information, of Australian social media users.

The Bill has been introduced ahead of the introduction of the full set of privacy reforms that the Australian Government committed to more than a year ago, in its response to the Attorney-General's Department Privacy Act Review report. The first tranche of reforms to the *Privacy Act 1988* (Cth) are currently before the Australian Parliament, but they do not address the vast majority of recommendations that the Government agreed to in whole or in principle. We urge the Government to commit to introducing the second tranche of Privacy Act reforms as soon as possible. Any age-restriction scheme will need to be underpinned by rigorous and consistent privacy protections, and many of the outstanding privacy reforms are key to addressing a range of harms that children and young people face online.[3]

Privacy concerns

Clause 63F(1)(b) of the Bill sets out privacy measures for social media entities to comply with when processing personal information for the purposes of restricting access. It provides that where an entity holds personal information about an individual that was collected with the purpose of preventing age-restricted users from accessing a social media account, the entity can only use or disclose this information in three circumstances: for the purposes of determining whether the individual is age restricted; with the consent of the individual; or *in circumstances where paragraph 6.2(b)(c) (d) or (e) of the Australian Privacy Principles apply* (cl 63F(1)(b)(ii)).

The application of the Australian Privacy Principles (APPs) in this context means that access to information would be permissible:

- Where it is required or authorised by a law or court (APP 6.2(b))
- Where a permitted general situation exists in relation to the use of disclosure of the information (APP 6.2 (c)). General situations include, for example, an entity having reason to suspect serious unlawful activity, or to lessen or prevent a serious threat to health.[4]
- Where a permitted health situation exists in relation to the use or disclosure of the information by the entity (APP 6.2(d)). This enables private entities and health services to use and collect information for identified health purposes relating to an individual.[5]
- Where the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 6.2(e)). An 'enforcement body' includes criminal law enforcement agencies such as police, and a range of other bodies at the state, territory and federal level with powers to issue civil penalties or sanctions, ranging from the Department of Home Affairs to Sports Integrity Australia. 'Enforcement related

[33] See HTI's submission to the Legal and Constitutional Affairs Committee Inquiry into the Privacy and Other Legislation Amendment Bill 2024 (October 2024).
[4] *Privacy Act 1988* (Cth) s 16A.
[5] *Privacy Act 1988* (Cth) s 16B.

activity' is a broad category that includes pursuing minor civil fines, and the prevention of minor crimes, such as speeding.[6]

The kinds of data collected under this clause, might, depending on the age-verification tool adopted, include a person's name, date of birth, sensitive biometric data (for facial recognition purposes), location data, the time and date of accessing a social media service, and potentially information drawn from a person's browser history that can be used to estimate their age. This is a significant, and sensitive, range of personal data that may be accessible under the Bill.

This personal data will be available to private sector or government entities that meet any of the broadly-defined circumstances listed above, in circumstances that may include, for example:

- Services Australia or the Australian Tax Office accessing information to investigate matters related to social security payments or taxation – such as in respect of parenting payments for carers, or child support (APP 6.2(e)).
- The Home Affairs Department accessing information about a person to investigate potential visa fraud (APP 6.2(e)).
- A social media company accessing information to establish or defend a legal or equitable claim against it (APP 6.2(c)).[7]
- A health service provider seeking access to information to conduct public health research in circumstances where the age of the information makes it impracticable to obtain consent, and where health research guidelines are complied with (APP 6.2(d).[8]

International human rights law provides that the right to privacy may be limited where it is a reasonable, necessary and proportionate means of fulfilling a legitimate purpose. Clause 63F(1)(b)(ii) will significantly increase intrusion on the right to privacy, in circumstances where this intrusion has *no connection* to the advancement of the legitimate purpose of the Bill itself – which is to protect children from the harms of social media. The privacy implications are all the more concerning because age-restriction processes would not be voluntary – it would be a requirement for access to social media services altogether. As such, HTI considers the provision to be an unjustifiable restriction on the human right to privacy.

Additionally, this provision is likely to undermine the success of the age-restriction scheme, which fundamentally relies on the Australian public trusting that their personal data will not be used for purposes beyond age verification. The level of access provided through the Bill is generalised and broad, to the point where over-use and mission-creep by government agencies is almost guaranteed, as we have seen in similar cases, such as in respect of metadata legislation, and COVID-tracing apps.[9] It is notable that the Albanese Government has committed to reforming metadata laws, including to address the level of access provided to

---

[6] *Privacy Act 1988* (Cth) s 6(1).

[7] Office of the Australian Privacy Commissioner, APP Guidelines: APP 6 Use or disclosure of personal information (July 2019) [6.39] <https://www.oaic.gov.au/__data/assets/pdf_file/0020/1199/app-guidelines-chapter-6-v1.1.pdf>.

[8] Office of the Australian Privacy Commissioner, APP Guidelines: APP 6 Use or disclosure of personal information (July 2019) [6.39] <https://www.oaic.gov.au/__data/assets/pdf_file/0020/1199/app-guidelines-chapter-6-v1.1.pdf> [6.50].

[9] Graeme Greenleaf and Katharine Kemp, 'Police access to COVID check-in data is an affront to our privacy. We need stronger and more consistent rules in place' The Conversation, 7 September 2021 < https://theconversation.com/police-access-to-covid-check-in-data-is-an-affront-to-our-privacy-we-need-stronger-and-more-consistent-rules-in-place-167360>.

non-criminal enforcement bodies.[10] Clause 63F(1)(b)(ii) in this Bill would create the same problem the Government is committed to addressing through metadata reform.

If Australians believe that age-restriction processes will be used significantly to chase fines, small debts and for other government (or commercial) purposes, rather than as a way to implement age restrictions, they are likely to lose trust in the scheme, and in the Australian Government's communications regarding the scheme. This could encourage people to circumvent the operation of the scheme, such as by adopting VPNs that mask the location of internet users and thus the legal requirements applicable to them. The public outcry in response to overly permissive data-sharing provisions in the My Health Record scheme, and subsequent opt-outs, is also instructive here.[11]

Proposed amendment

HTI recommends that clause 63F(1)(b)(ii) be removed from the Bill entirely. The only legitimate purpose for accessing personal data without consent in this context, would be to address issues with the technical functioning of the age-verification process itself (such as in respect of cyber-security issues or malfunctions), as this is important to the workability of the scheme. A provision to this effect could replace the current provision.

In the alternative, and only in the event that the Government advanced a compelling national security or community safety justification, clause 63F(1)(b)(ii) could be amended so that it enables access to personal information in a way that is proportionate to the relevant law enforcement imperative. This would mean that access to personal information from this scheme would be available only to such law enforcement bodies, such as the Australian Federal Police, that truly need access to it, and only in circumstances where these bodies have obtained independent authorisation for the investigation of a serious criminal offence.

In other words, access to personal information in this legislative scheme should be government by a system of judicial warrants, or warrants issued by a judge or magistrate acting persona designata. A 'serious offence' should be understood to meet the definition of 'serious offences' in section 5D of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act). The TIA Act regulates access to communications information by law enforcement bodies via warrants and the definition is transferable to the age-verification context.

Recommendation

- **Clause 63F(1)(b)(ii), which enables disclosure of personal information in circumstances where paragraph 6.2(b)(c) (d) or (e) of the Australian Privacy Principles apply, should be removed from the Bill. It should be replaced with a narrow provision enabling access to data for the purposes of addressing technical problems with the relevant age-restriction tool.**

[10] The Hon Mark Dreyfus KC MP, 'Government commits to significant metadata reforms' (Media Release, 21 February 2023) <https://ministers.ag.gov.au/media-centre/government-commits-significant-metadata-reform-21-02-2023>.

[11] See, e.g., Sophie Scott, Ariel Bogle and Laura Gartly 'My Health Record deadline looms, with privacy experts and Government at odds' *ABC News* (Online) 30 January 2019 <https://www.abc.net.au/news/2019-01-30/my-health-record-deadline-looms-jan-31/10759956>.

- **In the alternative, and provided the Government advanced a compelling national security or community safety justification, clause 63F(1)(b)(ii) should be amended to provide that personal information collected for the purposes of age restriction should only be disclosable where independent authorisation is provided to a law enforcement body in relation to a serious criminal offence, adopting the definition of 'serious offences' in section 5D of the *Telecommunications Interception and Access Act 1979* (Cth).**

Yours faithfully,

Edward Santow
Co-director, Human Technology Institute
Industry Professor – Responsible Technology

Sarah Sacher
Policy Specialist
Human Technology Institute