Input to the Statutory Review of the Online Safety Act 2021

June 2024

The Internet Society appreciates the opportunity to contribute to the statutory review of the Online Safety Act 2021.

The Internet Society is a global charity and nonprofit organization that supports and promotes the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society.

This document outlines and articulates our main points of concern. We hope that our submission will help the Australian government advance online safety expectations that uphold the ability of all Australians to continue to fully use and benefit from the open, global, and secure Internet.

We strongly urge the Australian government to amend the Online Safety Act to add:

> Section 24A: Nothing in this Act should cause services to weaken the security or confidentiality of encrypted communications or stored data.
>
> Section 145(1C): The Commissioner must not determine a standard under subsection (1) that requires or otherwise encourages or causes participants in an online industry to engage in scanning of the content of end-to-end encrypted communications.

Omission in the Current Regulatory Approach

The Australian regulatory approach to online safety (embodied in the Online Safety Act 2021 and its subordinate legislation and regulations) has put Australia on a path towards online *un-safety* by:

- neglecting to protect private communications from scanning; and
- proposing mandatory industry standards where services could be obliged to undertake client-side scanning of end-to-end encrypted communications, unless it is not technically feasible.

This regulatory approach fails to recognize the increasingly crucial role that end-to-end encryption plays in providing online safety, especially to "the most vulnerable members of society"[1] including children. It has also failed to give Australian users confidence that their private communications, protected by end-to-end encryption, will not be surveilled by services or the government.

Nobody would want to return to a time when websites used HTTP without the protection of Transport Layer Security (TLS) encryption. During that time, anyone with access to the networks between users and websites could observe and intercept sensitive information shared with schools, medical providers, financial institutions, and others. Therefore, today now that we have these basic protections, we should demand nothing less than secure end-to-end encryption for online communications. End-to-end encryption is an important preventative tool.

The online safety of millions of Australians depends on their ability to communicate confidentially, with the reassurance that their end-to-end encrypted communications and data are secure from surveillance, intrusion, and data breaches. End-to-end encryption protects the individuals and companies using the Internet and the Australian economy as a whole.

Children, for example, need encryption to communicate privately and safely with family, friends, teachers, and their doctor. End-to-end encrypted services protect their communications from being used for advertising, stolen in a data breach, or modified during transmission. This prevents service providers from using their content to train AI services or target them with personalized and potentially harmful ads.

All Australians need secure and trusted ways to communicate personal and sensitive information, including medical, employment, education, and financial data.

Survivors of domestic violence and other abuse, including children, depend on end-to-end encrypted technologies to communicate confidentially with trusted individuals, organizations, and sources of help and advice. Confidential communication provides a secure way for at-risk individuals to get support or relocate, protect the integrity of evidence, and prevent unauthorized access.[2] Confidentiality is also essential for the LGBTQ+ community, including youth, to exercise the right to live their truth without fear of persecution.[3]

---

[1] In 2022, the House of Representatives Select Committee on Social Media and Online Safety said:
"Australia, alongside the rest of the world, must address the causes and amplifiers of harm to ensure a safe and equitable [I]nternet, especially to the most vulnerable members of society."
House of Representatives Select Committee on Social Media and Online Safety, Social Media and Online Safety, March 2022, https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Social_Media_and_Online_Safety/SocialMediaandSafety/Report

[2] Understanding encryption: The Connections to Survivor Safety, US National Network to End Domestic Violence and the Internet Society, 2021, https://www.internetsociety.org/wp-content/uploads/2021/05/NNEDV_Survivor_FactSheet-EN.pdf

[3] Encryption: Essential for the LGBTQ+ Community, LGBT Tech and the Internet Society, 2019, https://www.internetsociety.org/wp-content/uploads/2019/11/Encryption-LGBT-Perspective-Fact-Sheet-EN.pdf

The push to make it easier for law enforcement to access the contents of end-to-end encrypted communications for investigations and prosecutions, after harm has already happened, puts at risk the ability of children, parents, social media, and others to use encryption effectively to protect people and prevent abuse.

The Online Safety Act 2021 does not include a clear statement that there is no requirement or expectation that services will take any action that could have the effect of breaking, weakening or otherwise undermining the encryption or other security tools and techniques used by services or their users. While not perfect, at least the recently proposed Canadian Online Safety Bill places private communications firmly out of scope and does not impose an overarching duty to scan all content on platforms[4].

The Australian online safety regulatory approach should be actively discouraging services from taking any action that could create or cause a security vulnerability. Further, it should be clear that end-to-end encrypted electronic services are not required or expected to implement scanning of the content of their users' messages or uploaded content, and that device and operating system developers are not required or expected to implement scanning of users' messages or uploaded content.

End-to-end encryption provides a technical guarantee that the message's contents are *confidential* between the sender and recipient and have not been altered or tampered with. Adding content scanning before a message is encrypted or after it is decrypted removes the confidentiality and integrity that users legitimately expect.[5] The same legitimate expectation applies to end-to-end encryption in other contexts, such as backups to "the cloud": the data should remain accessible only to the individual whose data is backed up, even if the backup is stored on a service provider's systems.

Scanning content on users' devices or apps is a violation of confidentiality, whether it happens before the data is encrypted, while it is encrypted, or after it has been decrypted. It's like having a surveillance camera watching over your shoulder as you write and receive messages. All users, including children, have a right to privacy and an expectation that a service that offers end-to-end encryption will not compromise the confidentiality or integrity of their communications or data.

If end-to-end encrypted services are required to use client-side scanning, users will no longer be able to have private and secure communications on those services. This could also lead to a higher risk of using "alternative services" for private communications, which may expose users to malware, data theft, and other potential risks. Encryption, including end-to-end encryption, is an essential digital

[4] What Governments Can Learn from Canada when Regulating Online Harms, Andrew Sullivan, President and CEO of the Internet Society, 18 March 2024 https://www.internetsociety.org/blog/2024/03/what-governments-can-learn-from-canada-when-regulating-online-harms/

[5] Client-Side Scanning: What It Is and Why It Threatens Trustworthy, Private Communications, Internet Society, updated 2022, https://www.internetsociety.org/wp-content/uploads/2020/03/2022-Client-Side-Scanning-Factsheet-EN.pdf

safety tool for children, parents, older people, vulnerable communities, and all Australians *because it ensures confidentiality and integrity*.

The Scope of the Review

We are concerned that the scope of the review casts end-to-end encryption, at best, as an obstacle to addressing online harms, or worse, as a contributing factor to online harm, with the Terms of Reference[6] asking:

> "Whether additional arrangements are warranted to address online harms not explicitly captured under the existing statutory schemes, including: ... (e) potential online safety harms raised by a range of emerging technologies, including but not limited to:
>
> - end-to-end encryption ..."

In our view, a more appropriate question would be:

> "Recognizing the increasingly widespread use of end-to-end encryption for online communications, how could we address online harm while preserving the security and confidentiality benefits of end-to-end encrypted services?"

Privacy

Speaking with respect to end-to-end encryption, the Issues paper[7] notes that the House of Representatives Select Committee on Social Media and Online Safety in 2022 concluded that "while privacy concerns are critical to the rights of all internet users, those issues did not 'outweigh the fundamental issue of ensuring safety in online environments".[8] Yet this statement fails to appreciate that privacy is a way of ensuring safety in the online environment because it prevents information from being misused against individuals, and that end-to-end encryption provides a technical guarantee that the information cannot be misused by others.

Further, one of the key findings of the Office of the Australian Information Commissioner (OAIC) Australian Community Attitudes to Privacy Survey 2023[9] was:

---

[6] Terms of Reference – Statutory Review of the *Online Safety Act 2021* https://www.infrastructure.gov.au/department/media/publications/terms-reference-statutory-review-online-safety-act-2021

[7] Statutory Review of the Online Safety Act 2021 Issues paper - https://www.infrastructure.gov.au/sites/default/files/documents/online-safety-act-2021-review-issues-paper-26-april-2024.pdf

[8] Parliament of the Commonwealth of Australia, House of Representatives Select Committee on Social Media and Online Safety, 'Social Media and Online Safety' March 2022 https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Social_Media_and_Online_Safety/SocialMediaandSafety/Report

[9] https://www.oaic.gov.au/__data/assets/pdf_file/0025/74482/OAIC-Australian-Community-Attitudes-to-Privacy-Survey-2023.pdf

> "Protecting their child's personal information is a major concern for 79% of parents. However, only half feel they are in control of their child's data privacy. Eighty-five per cent of parents believe children must be empowered to use the internet and online services, but their data privacy must be protected."[10]

International Approaches

Respecting human rights

Children have a right to privacy. Article 16 of the United Nations Convention on the Rights of the Child states: "No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor unlawful attacks on his or her honor and reputation."

Encryption enables children to exercise their right to privacy. It also enables services that collect, communicate, or store information about children to protect their privacy. Encryption guarantees confidentiality and message integrity, safeguarding children's online interactions and personal safety.

We recommend the review carefully consider the rights of the child, including their right to privacy.

Safety by design

The concept of "safety by design" outlined in the Issues paper[11] "... focuses on the ways that technology companies can minimise online threats by anticipating, detecting and eliminating online harms before they occur". But another essential aspect of safety by design is prevention. End-to-end encryption provides safety by design by preventing third party access to readable, and, therefore, usable content. There are other safety by design technologies and strategies that the review could consider that do not depend on detection of harm via detection of content.

A statutory duty of care

Unintended and perverse consequences could arise with the introduction of a statutory duty of care, causing service providers to engage in invasive surveillance of their users and censorship of legitimate content. The concept could also be stretched to force service providers to remove or refrain from implementing end-to-end encryption, jeopardizing their users' security, privacy and safety.

Supporting users

As much as possible, we believe it is important to allow end-users to control what content they wish to see and how they send or receive it, recognizing that services also have a role in deciding what

[10] Data breaches seen as number one privacy concern, survey shows, OAIC media release, 8 August 2023, https://www.oaic.gov.au/newsroom/data-breaches-seen-as-number-one-privacy-concern-survey-shows

[11] Statutory Review of the Online Safety Act 2021 Issues paper - https://www.infrastructure.gov.au/sites/default/files/documents/online-safety-act-2021-review-issues-paper-26-april-2024.pdf

services they want to provide and how they will be used. Taking this approach increases end-user trust and empowerment in online participation.

User controls are important tools, not only for users to manage their access to content, but also to adjust preferences in the service, use assistive technologies, communicate privacy consent/non-consent and other permissions to service providers, and other aspects of how they use the service. Best practices in user controls are not static, and evolve with experimentation and user testing.

A vital safety user control is end-to-end encryption. Services that offer end-to-end encryption give end-users control over the security of their communications and online safety by protecting the confidentiality and integrity of their communications.

Blocking content

In line with the reasons for judgment of The Honourable Justice Kennett in *eSafety Commissioner v X Corp [2024] FCA 499*, the Online Safety Act should be clear that the eSafety Commissioner's powers do not extend extraterritorially, and accordingly, for example, that any removal, remedial or link deletion notices do not affect users outside of Australia under the jurisdiction of another country.

Recommendations

Based on the evidence we have shared, we strongly urge the Australian government to amend the Online Safety Act by adding the two following Sections:

1. Section 24A: Nothing in this Act should cause services to weaken the security or confidentiality of encrypted communications or stored data.
2. Section 145(1C): The Commissioner must not determine a standard under subsection (1) that requires or otherwise encourages or causes participants in an online industry to engage in scanning of the content of end-to-end encrypted communications.

Thank you for taking public comment for the statutory review of the Online Safety Act 2021 and considering our input. We would happily elaborate on our contribution.