Input to Online Safety (Basic Online Safety Expectations) Amendment Determination 2023

The Internet Society appreciates the opportunity to contribute to the Online Safety (Basic Online Safety Expectations) Amendment Determination 2023.

The Internet Society is a global charity and non-profit 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 Department of Infrastructure, Transport, Regional Development, Communications and the Arts ("the Department") to add in Schedule 1 section 1:

> Additional expectation (2B)
>
> The provider of the service is not required to take any action that could have the effect of weakening or otherwise undermining the encryption or security of its service.
>
> Additional expectation (2C)
>
> The provider of an end-to-end encrypted electronic service is not required to implement client-side scanning.

In Schedule 1 section 4, to add to paragraph (6):

> (d) making available end-to-end encryption for users.

In Schedule 1 section 6, insert:

> Nothing in this instrument weakens the protections of Australian Privacy Principle 2.1 (Schedule 1 of the Privacy Act 1988).

End-to-end encrypted services

The online safety of millions of Australians depends on their ability to communicate confidentially, confident 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 service and the Australian economy as a whole.

Children, for example, need the confidentiality of encryption to communicate privately and safely with family, friends, teachers, and their doctor. End-to-end encrypted services protect their communications from being monetized for advertising or stolen in a data breach. It prevents service providers from using their content to train AI services or target them with personalized 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.[1] Confidentiality is also essential for the LGBTQ+ community, including youth, to exercise the right to live their truth without fear of persecution.[2]

The Online Safety (Basic Online Safety Expectations) Determination 2022 and the proposed Online Safety (Basic Online Safety Expectations) Determination 2023 ("the Determination") do not articulate how the basic online safety expectations should be applied to encrypted services, particularly those with end-to-end encryption.

We strongly urge the Department of Infrastructure, Transport, Regional Development, Communications and the Arts ("the Department") to clarify in the Determination 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 the service or its users. Indeed, the Determination should be clear that services are discouraged from taking any action that could create or cause a security vulnerability.

Further, the Determination should also state that end-to-end encrypted electronic services are not required or expected to implement server-side or client-side scanning of the content of their users' messages or uploaded content and, similarly, that device and operating system developers are not required or expected to implement server-side or client-side scanning of users' messages of 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

[1] 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

[2] 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

integrity that users legitimately expect.[3] 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.

Encryption, including end-to-end encryption, is an essential digital safety tool for children, parents, older people, vulnerable communities, and all Australians *because it ensures confidentiality*.

User controls

We welcome the expectation that electronic services will take reasonable steps to make controls available to end-users to exercise choice and autonomy over the content they receive or view, and note that smaller or new entrants may not be able to offer the full range of controls that a large or dominant service provider could provide. 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 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. Considerable care should be taken not to be prescriptive as this could hinder or prevent the deployment of newer and better user controls.

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. Suppose end-to-end encrypted services are expected to implement client-side scanning. In that case, end-users will lose their ability to have confidential communications on those services and lose the ability to be confident that the communications have not been altered in transit. They lose their ability to have private communications.

[3] 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

Anonymous and pseudonymous accounts

We appreciate the challenges services and end-users face when bad actors repeatedly abuse services' terms of service and engage in harmful conduct through pseudonomyous or anonymous accounts. However, any reactive or proactive measures "to prevent the same person from repeatedly using anonymous accounts to post material, or to engage in activity, that is unlawful or harmful" must not undermine end-users' ability to interact with a service anonymously or pseudonymously. We are concerned that the expectation of proactive measures could encourage service providers to implement real-name policies or to require end-users to provide identifiers tied to their legal identity, such as phone numbers, a driver's license number, or credit card, when not strictly necessary. An end user's ability to interact with a service anonymously or pseudonymously is an important user safety control for their interactions within the service and for their offline safety. Even if an end-user's name is presented pseudonymously to other users, their legal identity might be exposed if a service provider collects identifying data leaked by an employee or contractor, deliberately or accidentally, or if a service is hacked. Also, once a service provider has such data, they might be tempted to use it for other purposes.

For the avoidance of doubt, the Determination should be clear that it does not weaken the protections of Australian Privacy Principle 2.1 (Schedule 1 of the Privacy Act 1988):

> "2 Australian Privacy Principle 2—anonymity and pseudonymity
>
> 2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

Appropriate age assurance mechanisms

The Department should not include the example of implementing appropriate age assurance mechanisms for the expectation that:

> "[t[he provider of the service will take reasonable steps to ensure that the best interests of the child are a primary consideration in the design and operation of any service that is used by, or accessible to, children"

in the Determination without clear guidance on what would or would not be appropriate after consultation with the community. Generally, it would not be in the best interests of a child to be identified or identified through a protected attribute such as race, disability, or gender to gain assurance as to their age. Further, parental assertion may not be appropriate, especially in circumstances where there is an abusive relationship. Care should also be taken to avoid encouraging service providers to use age assurance services that over-collect children's personal data and store it, possibly insecurely, and may even on-sell the data or use it for other purposes.

Thank you for taking public comment on the proposed Determination and considering our input. We would happily elaborate on these concerns.