Input to the Draft Industry Standards for Designated Internet Services and Relevant Electronic Services

The Internet Society appreciates the opportunity to contribute to the eSafety Commissioner's draft industry standards for Designated Internet Services and Relevant Electronic Services.

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 eSafety Commissioner advance industry standards that uphold the ability of all Australians to continue to fully use and benefit from the open, global, and secure Internet.

Overview

The draft standards may not directly mandate the technologies that electronic services must use to be in compliance. However, they would effectively require end-to-end encrypted electronic services to implement content scanning or other measures to detect and identify CSAM or pro-terror material *unless it is not technically feasible*.

Even if it were technically feasible, scanning end-to-end encrypted electronic services breaks the technical promise of content confidentiality, introduces pervasive surveillance, undermines the safety and security of millions of Australians, and significantly sets back Australia's goal of becoming a world leader in cyber security.

We are very concerned that the draft standards would weaken digital security in Australia, and we believe that they must not go forward without explicitly including, at a minimum, these crucial protections for encryption and its use:

- There must be no requirement for electronic services to 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,
- The standards should explicitly state that end-to-end encrypted electronic services are not required 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 to implement server-side or client-side scanning of users' messages of uploaded content, and
- Electronic services are not required to take and are discouraged from taking any action that could create or cause a security vulnerability in their service.

Further, the standards should explicitly state that something is not "technically feasible" if it would weaken the security of the service or integrity of users' data.

Scanning Breaks the Technical Promise of Confidentiality of End-to-End Encryption

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.[1] 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*.

Children 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.

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]

---

[1] 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

[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

Confidentiality is also essential for the LGBTQ+ community, including youth, to exercise the right to live their truth without fear of persecution.[3]

Even the Australian government depends on the same electronic services covered by the draft standards to communicate with citizens. As Signal highlighted in 2018:

> "... everyone benefits from these design decisions – including Australian politicians. For instance, it has been widely reported that Malcolm Turnbull, the 29th Prime Minister of Australia, is a Signal user. He isn't alone. Members of government everywhere use Signal. Even if we disagree with Christian Porter, we would never be able to access his Signal messages, regardless of whether the request comes from his own or any other government".[4]

Recognizing how vital it is to preserve the confidentiality of digital communications, the Civil Liberties Committee of the European Parliament on 14 November 2023 adopted a position excluding end-to-end encryption from the scope of the detection orders in the *proposed Regulation, laying down rules to prevent and combat child sexual abuse,* to guarantee that all users' communications are secure and confidential.[5]

Technical Feasibility Is Not a Sufficient Safeguard

The requirement for an electronic service to implement client-side scanning or other measures under the draft standards depends on whether it is technically feasible. However, just because something is considered "technically feasible" does not necessarily mean it will be functional, secure, or not cause harm. The standards should clearly state that an action is not "technically possible" if it could weaken the security of the service or the integrity of users' data. Additionally, any systems, processes, or technologies used to detect and identify content must be transparent, secure, reasonable, proportionate, and practical and should not undermine users' expectations of confidentiality and integrity.

Scanning Is Neither a Reliable nor Secure Option

Client-side scanning is neither a reliable nor a secure option for detecting and identifying illegal content in end-to-end encrypted services. It does not robustly achieve its primary objective of detecting known prohibited content, and its detection algorithms can be repurposed to add hidden secondary capabilities, covertly enabling surveillance and industrial espionage. This is the

[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

[4] Setback in the Outback, Signal blog post by Joshua Lund (jlund), 2018, https://signal.org/blog/setback-in-the-outback/

[5] European Parliament Press Release, Child sexual abuse online: effective measures, no mass surveillance, 14 November 2023, https://www.europarl.europa.eu/news/en/press-room/20231110IPR10118/child-sexual-abuse-online-effective-measures-no-mass-surveillance

overwhelming expert view of researchers and other technical experts in the fields of information security and cryptography.[6]

As the Steering Committee of the Global Encryption Coalition recently highlighted regarding the UK Online Safety Act, "safe versions of these scanning technologies do not exist and are unlikely to ever exist."[7] Further, research from Imperial College London concluded, "We don't understand the risks well enough to ask for the deployment of CSS [client-side scanning] technology on hundreds of millions of devices."[8]

The Internet Architecture Board ("IAB"), which provides long-range technical direction for Internet standards, ensuring the Internet continues to grow and evolve as a platform for global communication and innovation, emphasized in a recent statement:

> "For technologies where the intended purpose is scanning of user communication, there is by design no technical way to limit the scope and intent of scanning, nor curtail subsequent changes in scope or intent. Further, specifically when scanning for illegal content, transparency cannot be provided. Mandating such technologies impacts all users of the global Internet and creates a tool that is straightforward to abuse as a widespread facilitator of surveillance and censorship, presenting real-world dangers to the free flow of information and the security and privacy of people. Without privacy, users cannot benefit from the Internet's virtue to connect people and support freedom of expression".
>
> Additionally, one of the founding principles of the Internet has been its openness; the ability for any standards-compliant software to access the network of networks has been the catalyst for world-changing innovations over many decades. Mandatory use of client-side scanning, and the regulatory burden it would impose, would negatively impact this, restrict use of open-source software, and lead to a stagnant landscape where users lose choice".[9]

Even the UK Government's own Safety Tech Challenge Fund, which was supposed to identify safety scanning technologies, failed in its mission. The independent review by the UK's National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN) identified significant

---

[6] Open Letter from Security and Privacy Researchers in relation to the Online Safety Bill, undated https://haddadi.github.io/UKOSBOpenletter.pdf and Open Letter to UK Prime Minister expressing dangers of the UK's Online Safety Bill, 24 November 2022, https://www.globalencryption.org/2022/11/70-organizations-cyber-security-experts-and-elected-officials-sign-open-letter-expressing-dangers-of-the-uks-online-safety-bill/

[7] Global Encryption Coalition Steering Committee Statement on the UK's Online Safety Bill, The Center for Democracy & Technology, Global Partners Digital, the Internet Freedom Foundation, the Internet Society, and Mozilla, 20 September 2023, https://www.globalencryption.org/2023/09/steering-committee-statement-on-the-uks-online-safety-bill/

[8] Imperial College London News, Tech mandated via Online Safety Bill 'could turn phones into surveillance tools', by Laura Gallagher, Caroline Brogan, 19 May 2023, https://www.imperial.ac.uk/news/244952/tech-mandated-online-safety-bill-could/

[9] Internet Architecture Board (IAB) Statement on Encryption and Mandatory Client-side Scanning of Content, 15 December 2023, https://www.iab.org/documents/correspondence-reports-documents/2023-2/iab-statement-on-encryption-and-mandatory-client-side-scanning-of-content/

problems with proposed scanning technologies from that initiative, including that they would undermine end-to-end encryption.[10]

Additionally, scanning technologies produce false positive and false negative results. A technology that promises 99.99% accuracy may sound acceptable, but statistically, if applied to message volumes of 1 billion a day,[11] would result in 100,000 erroneous results daily. If human moderation cannot cope with that volume of errors, the system will result in unjust prosecutions and unprosecuted crimes. Technical viability cannot be gauged in isolation from a country's moderation and enforcement capacity.

Adverse Impact on the Australian Economy

In addition to significant compliance costs, the draft standards will likely cause adverse economic effects that will harm the Australian economy.

The Internet Society commissioned a team of independent researchers to assess the economic impact of TOLA. This team, Law & Economics Consulting Associates (LECA), published its final report—*The Economic Impact of Laws that Weaken Encryption* on 1 June 2021.[12] One Australian company responding to the researchers' survey and interviews estimated that the direct adverse economic impact of TOLA was around AU$ 1 billion.

The report on TOLA found that:

- The single most significant source of adverse economic effects is TOLA's indirect threat to trust in digital services, including the Internet.
- TOLA can potentially result in significant economic harm for the Australian economy and produce negative spillovers that will amplify that harm globally.
- TOLA has increased business uncertainty and can harm the brand image of designated communications providers with operations in Australia.
- In a survey of 79 companies, 54 of which are based in Australia, 36% of those whom the TOLA Act had impacted stated that TOLA has negatively impacted the risk environment for their business. And around 20% said the law had had a direct negative impact on their business. A further 21% believed that TOLA would negatively impact the future operating costs of their business, including compliance and remediation.

[10] REPHRAIN: Towards a Framework for Evaluating CSAM Prevention and Detection Tools in the Context of End-to-end encryption Environments: a Case Study, Claudia Peersman, José Tomas Llanos, Corinne May-Chahal, Ryan McConville, Partha Das Chowdhury and Emiliano De Cristofaro, February 2023, https://bpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/1/670/files/2023/02/Safety-Tech-Challenge-Fund-evaluation-framework-report.pdf

[11] In 2020, WhatsApp alone was processing over 100 billion messages a day, worldwide—up from 60bn in 2016, and one billion in 2010.

[12] The Economic Impact of Laws that Weaken Encryption, By George Barker, William Lehr, Mark Loney, and Douglas Sicker, 5 April 2021 - https://www.internetsociety.org/wp-content/uploads/2021/05/The_Economic_Impact_of_Laws_that_Weaken_Encryption-EN.pdf

These findings indicate that the draft standards also risk adversely affecting the Australian economy, first, by creating legal uncertainty as to what would be sufficient for compliance (especially for detecting and identifying CSAM). Second, it makes businesses uncertain whether modifying their products and services will affect revenues in Australia and other markets. Third, by lowering trust in the security and trustworthiness of electronic services that would be required to comply with the draft standards.

Even the prospect that designated communications providers could be required to build-in access for law enforcement in their services has resulted in significant economic harm. We must assume that mandating scanning for illegal material in end-to-end encrypted communications will have similar adverse economic effects.

Implications for Australia's Cybersecurity

On 22 November 2023, the Australian Government released the 2023-2030 Australian Cyber Security Strategy, a "roadmap that will help realize the Australian Government's vision of becoming a world leader in cyber security by 2030", and an accompanying Action Plan.[13] If Australia does require end-to-end encrypted services to implement client-side scanning, it would become a world leader *in cyber insecurity*. According to security experts, client-side scanning ("CSS"):

> *"... neither guarantees efficacious crime prevention nor prevents surveillance. Indeed, the effect is the opposite. CSS, by its nature, creates serious security and privacy risks for all of society, while the assistance it can provide for law enforcement is, at best, problematic. There are multiple ways in which client-side scanning can fail, can be evaded, and can be abused."*[14]

The experts' analysis is not merely a commentary on technical feasibility: if technical enforcement measures are ineffective, then by definition, they will fail the necessity and proportionality tests that protect against violations of fundamental rights.

Conclusion and Recommendations

Conclusion

The proposed standards significantly threaten the public's ability to communicate confidentially. This is especially problematic in a society that relies heavily on information in a data-driven economy, as it will hinder the exercise of fundamental rights and personal autonomy. Additionally, these proposals

[13] See Department of Home Affairs website at https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

[14] Bugs in Our Pockets: The Risks of Client-Side Scanning, Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague, Carmela Troncoso, 14 October 2021, https://www.cs.columbia.edu/~smb/papers/bugs21.pdf

risk harming citizens' and businesses' ability to safely participate in the digital economy, which could negatively affect Australia and its regional partners.

Recommendations

The draft standards must not go forward without explicitly including these crucial protections for encryption and its use:

- There must be no requirement for electronic services to 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,
- End-to-end encrypted electronic services are not required to implement server-side or client-side scanning of the content of their users' messages or uploaded content,
- Similarly, device and operating system developers are not required to implement server-side or client-side scanning of users' messages of uploaded content and
- Electronic services are not required to take and are discouraged from taking any action that could create or cause a security vulnerability in their service.

Thank you for taking public comment on the draft standards and for considering our input. We would happily elaborate or speak to your office about these concerns.