Global Encryption Coalition

Joint Submission to the Industry Standards Consultation

20 December 2023

//

Dear Commissioner Inman Grant,

We the undersigned organisations and individuals urge you to protect the privacy and security of communications and cloud file storage for internet users.

We acknowledge the severity of harm caused by the dissemination of child sexual abuse material (CSAM) and other forms of illegal content, and we support strong regulation to ensure platform accountability, the empowerment of users as well as the protection of their rights and safety. It is essential that governments, with the support of industry, take effective steps to regulate the spread of illegal content. It is also essential that such approaches do not also disproportionately lead to the creation and exacerbation of other harms, and adopt best practices in international policy making.

The eSafety Commissioner has proposed two draft industry standards[1] (1) under the Online Safety Act. Taken together, these standards apply to a broad range of services that people use every day including email, text and instant messaging, video communications, online gaming, dating services, and online file storage. In a context in which cybersecurity risks are rising, the safety, rights, and wellbeing of individuals and communities rely on the digital security and the privacy of these services.

Both draft standards include a range of proactive detection obligations on digital services to scan content in order to detect, remove, disrupt and deter CSAM and 'pro-terror' content. There are no specific safeguards for end-to-end encrypted services that people rely on for privacy and safety, as content on such platforms cannot be accessed by any third party, including the service provider, at any stage of the communication/storage process. Hashing and artificial intelligence technologies are specifically referenced to detect and remove objectionable content. Such approaches, when deployed on a device, are commonly referred to as 'client side scanning.' These methods have been widely criticised by privacy and security researchers, digital rights advocacy organisations and human rights groups around the world.[2] Internet safety advocates and child rights groups have emphasised the importance of looking at other methods to enhance online safety for children and minimise the dissemination of CSAM, and how encryption works to protect the rights of children.[3] Scanning technologies are deeply flawed because they: have questionable effectiveness;

[1] See two draft industry standards: https://www.esafety.gov.au/industry/codes/standards-consultation

[2] See, for example, this open letter in response to the EU's proposed Child Sexual Abuse Regulation, signed by over 450 scientists and researchers: https://docs.google.com/document/d/13Aeex72MtFBjKhExRTooVMWN9TC-pbH-5LEaAbMF91Y/edit

[3] See, for example, 'Privacy and Protection: A children's rights approach to encryption,' Child Rights International Network, 19 January 2023, which concludes technologies including client-side scanning is akin to breaking encryption by compromising its aims, and points to other underutilised safety mechanisms such as user reporting, https://home.crin.org/readlistenwatch/stories/privacy-and-protection; and 'Chat Control or Child Protection?' Ross Anderson, Foundation for Information Policy Research, October 2022 which notes alternative methods to tech solutionism to enhance safety, https://www.cl.cam.ac.uk/~rja14/Papers/chatcontrol.pdf.

contain a high risk of false positives; increase vulnerabilities to security threats and attack – thereby weakening online safety for all users – and enable the ability to expand use of such systems to scan other categories of content in the future.[4]

The eSafety Commissioner has publicly stated that it supports privacy and security, and does not advocate building in weaknesses or back doors to undermine end-to-end encrypted services.[5] But client-side scanning fundamentally undermines encryption's promise and principle of private and secure communications and personal file storage. We urge the Commissioner against creating standards that would force encrypted services to implement such scanning measures as they would create an unreasonable and disproportionate risk of harm to individuals and communities.

Australia is a leader in the field of online safety policy making, and this position comes with responsibility in shaping the norms and direction of international internet governance and regulation. Proceeding with the standards as drafted would signal to other countries that online safety is somehow counterposed to privacy and security, when the opposite is true.

We strongly urge the eSafety Commissioner to amend the proposed industry standards to ensure the protection of privacy and security, and urge the Australian Government to commit to the ongoing protection and strengthening of encryption, privacy and digital security.

Sincerely,

The following undersigned organisations and individuals,

[4] For further detail on the risks of client side scanning see: 'Fact Sheet: Client-Side Scanning', Internet Society 24 March 2020, https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/; and 'Bugs in our Pockets: The Risks of Client-Side Scanning,' 14 October 2021, https://arxiv.org/abs/2110.07450.

[5] See 'Updated Position Statement: End-to-end encryption ,' October 2023 https://www.esafety.gov.au/sites/default/files/2023-10/End-to-end-encryption-position-statement-oct2023.pdf; and 'Australia releases new online safety standards to tackle terror and child sexual abuse content,' The Guardian, 20 November 2023, https://www.theguardian.com/australia-news/2023/nov/20/australia-esafety-standards-new-2023-targets-child-content-terrorism-detection.

Organisations

Note 1: eSafety has redacted the names of 40 organisation signatories

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Individuals*

*Affiliation for identification purposes only

Note 2: eSafety has redacted the names of 565 individual signatories

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted] [redacted]