Electronic Frontiers Australia

Electronic Frontiers Australia Inc.
ABN: 35 050 159 188
W www.efa.org.au
E email@efa.org.au

MS J Inman-Grant

eSafety Commissioner

Canberra ACT 2610

16 December 2023

By email

Dear Ms Inman-Grant,

RE: Draft On-line Industry Standards for Relevant Electronic Services ('RES') and Designated Internet Service ('DIS') Codes.

Background

The Board and membership of EFA are strongly concerned about elements of the proposed Industry Standards for RES and DIS Codes. In particular we are deeply worried by the potential for undermining the privacy, safety and security of encrypted communications and cloud file storage for internet users.

EFA acknowledges the severity of harm caused by the dissemination of child sexual abuse material (**'CSAM'**), pro-terror material and other forms of illegal content. We support strong regulation to ensure platform accountability, the empowerment of users as well as the protection of digital privacy and other human rights, welfare, security and safety for all individuals.

EFA Response

EFA recognizes that it is essential for governments, with the support of industry, to take effective steps to regulate the spread of illegal content. It is also equally essential that such regulatory approaches do not disproportionately and unnecessarily lead to the creation and exacerbation of other serious societal and individual harms at the expense of our inherent human and digital rights. Such an outcome would create a surveillance state which treats all on-line users as 'suspects first' and not citizens with inherent human and digital rights. Further, it would make a trusted, safe and secure online environment untrustworthy, unsafe and vulnerable to both bad actors and further regulatory overreach.

The eSafety Commissioner has proposed two draft Industry Standards **(1)** under the *Online Safety Act (Cth) 2021*. 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.

Undermining of Privacy Enhancing Technology

In a context in which cybersecurity risks are continually increasing, our privacy laws remain inadequate and not fit for purpose by not keeping pace with technology, the proposed Industry Standards are both Orwellian by design and effect. The safety, rights and wellbeing of individuals and communities and their willingness to engage in digital services all depend on the security and privacy capabilities provided by online service providers, of which end to end encryption - a "***Privacy Enhancing Technology***" - is a key foundational capability. Undermining this capability increases the risk of harm, diminishes trust in on-line service providers, disproportionately impacts vulnerable user groups and can be incredibly detrimental to the digital economy and peoples' participation therein.

Both draft Industry Standards include a range of proactive detection obligations on digital service providers 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 security, 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. This degree of privacy, safety and security is fundamental to individuals trusting both the platform and service provider.

Client Side Scanning and Use of Artificial Intelligence

The draft Industry Standards specifically reference the use of artificial intelligence technologies to detect and remove objectionable or unlawful 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)** EFA is strongly supportive of this position.

Client side scanning technologies remain deeply flawed because they: have questionable effectiveness; 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 the government or regulator of the day to expand use of such systems to scan other categories of content in the future. **(4)**

Inconsistent Positioning on Client Side Scanning

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. When considering the specific language concerning the obligation for client side scanning in the 2 Industry Standards the position taken by the eSafety Commissioner seems both contradictory and a non sequitur.

EFA’s Request

EFA and its members strongly urge the eSafety Commissioner **against** creating standards that would force certain encrypted service providers to implement such scanning measures as they would create an unreasonable and disproportionate risk of harm to all individuals and communities who participate in these on-line services. It effectively treats all citizens as suspects and diminishes the integrity and trustworthiness of multiple digital ecosystems.

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 two Industry Standards as drafted would signal to other countries that online safety is somehow counterposed to privacy and security, when the opposite is true. Privacy and on-line safety are not zero sum propositions.

EFA’s Recommendations

EFA strongly supports global efforts to prevent and reduce the dissemination of CSAM and pro-terror material. However, the track record of this approach shows it has not had the success predicted and erodes the privacy, safety and security of the broader population and potentially also vulnerable sub-populations.

EFA considers that other holistic approaches and methodologies outside of technology driven solutions must be pursued first. This includes:

- More CSAM research
- Acting on existing research that calls for easier reporting as a priority

- Ensuring that any attempt to reduce dissemination of CSAM and pro-teror material must not minimise awareness of the circumstances that the content is created and released online
- Providing greater education to the public, especially for parents and children
- Introducing well designed regulation for platforms operating in the digital adult entertainment industry which promote material termed as "teen" , "barely legal" or "young" or host similarly themed live streaming services.
- Ensuring future regulatory obligations for on-line platforms include requirements to have sufficient resourcing and tooling to identify CSAM and pro-terror material and report it to relevant legal authorities.

To ensure the continued privacy, safety and security of the entire Australian on-line community and that on-line services remain trustworthy we strongly urge the eSafety Commissioner to amend the two proposed Industry Standards by removing any express or implied obligation to undertake client side scanning or circumvent end to end encryption in on-line services. We further urge the Australian Government to openly commit to world leading practices for the ongoing protection and strengthening of encryption, privacy and digital security for all Australian citizens.

Yours sincerely,

John Pane
Chair
Electronic Frontiers Australia

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.

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.

About EFA

Established in January 1994, EFA is a national, membership-based, not-for-profit organisation representing Internet users concerned with digital freedoms and rights.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political, and civil liberties issues involved in the use of digital communications systems.