Executive Manager
Office of the safety Commissioner

By Email: submissions@esafety.gov.au

Date	21 December 2023
Reference	Draft Standards Designated Internet Services Relevant Electronic Services

Internet Australia appreciates the opportunity to comment on the draft Standards covering Designated Internet Services and Relevant Electronic Services. Internet Australia agrees with the basic premise of these standards: that steps must be taken to address the growing amount of harmful material that is available online, and that the participants in that industry must play a role in addressing that issue. Indeed, many of the steps proposed in the standards will play an important part in combatting the rise of harmful material online.

Internet Australia does, however, have concerns about both Standards. The Standards require what amounts to having visibility of message content which will undermine the confidence that both business and public have in the privacy of their communications. We are also concerned that some of the measures proposed may not be effective. Further, many smaller industry providers may be required to undertake processes that could be a significant burden. Finally, the law now allows law enforcement agencies to undertake interception activities – all of which require legal oversight and reporting. We would not support any standard that allows industry to carry out what could amount to interception of communications outside of what is allowed by law.

About Internet Australia

Internet Australia is the not-for-profit organisation representing all users of the Internet. Our mission – "Helping Shape Our Internet Future" – is to promote Internet developments for the benefit of the whole community, including business, educational, government and private Internet users. Our leaders and members are experts who hold significant roles in Internet-related organisations and enable us to provide education and high-level policy and technical information to Internet user groups, governments and regulatory authorities. We are the Australian chapter of the global Internet Society, where we contribute to the development of international Internet policy, governance, regulation and technical development for the global benefit.

Holly Raiche, Policy Chair, Internet Australia

Most of the ‘compliance measures’ required in Part 4 of both Standards are reasonable steps that relevant industry members should take to address harmful online material. These include the following:

- Having terms of use that prohibit the use/display of such material, reporting material to the relevant authorities and terminating the service of those who have contravened such terms of use
- Providing or providing access to educational material on possible steps to address harmful material
- Providing regular reports to the relevant authority on harmful material, etc.

Our specific concerns with the proposed ‘compliance measures’ concern the implications for privacy, particularly the privacy rights of children; the effectiveness of some of the measures proposed; and impact of Standards’ requirements on smaller industry members covered by these Standards.

Interception and Privacy

The Discussion Paper accompanying the release of both Standards makes it clear that the Standards “do not require encryption to be weakened or subverted’[1]. The requirements only apply ‘if is technically feasible for the service to detect and remove material’.[2] While that statement is welcome, its clear implication is that if it IS technically feasible then the industry participant must do what is required.

The language of both Standards is that ‘if is technically feasible, the industry participant … ‘must implement systems, processes and technologies that detect and identify….[3] What is implied is what is called ‘client side scanning. The term refers to systems:

> … that scan message contents – i.e., text, images, video files – for matches or similarities to a database of objectionable content before the message is sent to the intended recipient.[4]

[1] Discussion Paper 12-13.

[2] Ibid

[3] Clauses 21-23 in the Standard for Designated Internet Services and Clauses 20-22 of the Standard for Relevant Electronic Services.

[4] Internet Society, *Client-Side Scanning: What It Is and Why It Threatens Trustworthy, Private Communications,* August 2022. For an explanation of how client-side scanning works, see pp 2-3.

As that fact sheet explains:

> This fundamentally defeats the purpose of E2E encryption. Private and secure E2E encrypted communications between two parties, or among a group, are meant to stay private. If people suspect their content is being scanned, they may self-censor, switch to another service without client-side scanning or use another means of communication.[5]

A recent Report from Child Rights International Network[6] highlights the special issues raised for children by the use of techniques including client side scanning, particularly in the name of child protection. The Report was written in response international legislation in the US[7] the UK[8] and the EU[9]. After a fulsome discussion on the techniques of encryption and their implications, the paper asks:

> Who may interfere with a child and their full and free development, their everyday activities and communications, how and with what effect, and for what purposes?[10]

The paper explores numbers of situations where children's use of insecure communications has led to unauthorised people having access to children's communications. And sadly, the paper includes situations where even family access to a child's communications may create conflict.[11] The paper, quoting the UN Committee on the Rights of the Child, then provides detailed arguments to support that 'privacy is vital to children's safety.[12]

[5] Ibid

6 Child Rights International Network (**CRIN**), Privacy and Protection: *A Children's Rights approach of Encryption*, 2023 < https://home.crin.org/readlistenwatch/stories/privacy-and-protection>. See also *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.>

[7] EARN IT Act of 2022< https://www.congress.gov/bill/118th-congress/senate-bill/1207>

[8] Online Safety Bill <https://bills.parliament.uk/bills/3137>

[9] EU proposed Child Sexual Abuse Regulation <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN>

[10] CRIN 28

[11] Ibid 29

[12] Ibid 52, quoting from the UN Committee on the Rights of the Child, General Comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/G//GC/25, 2 March 2021.

Effectiveness of Proposed Measures

As noted above, Australia is not the only jurisdiction to propose legislation calling for greater protection for online activities, particularly for Children.[13] While each of the Bills differ in requirements on the measures industry will be required to take, they all have requirements that, in various ways, would require industry members to detect harmful online material.

Perhaps the clearest criticism of such legislation came from a letter to the European Parliament and EU states, signed by over 450 scientists and researchers from 38 countries. [14] The signatories began by acknowledging that child sexual abuse and exploitation is a serious crime and that the responsibility of governments is to take effective measures to both prevent and react quickly to such criminal behaviour. However, they are highly critical of the steps required by the EU Regulation which include scanning of messages, pictures, text, voice mail and, for E2E material, client-side scanning. In their view:

> … such undermining will weaken the environment for security and privacy work in Europe, lowering our ability to build a secure digital society. … and set a global precedent for filtering the Internet, controlling who can access it, and taking away some of the few tools available for people to protect their right to a private life in the digital space. This will have a chilling effect on society and is likely to negatively affect democracies across the globe.[15]

.

Their comments are divided into three sections. The first – "Detection technologies are deeply flawed and vulnerable to attacks' – explains in detail why tools use for scanning can be easily changed both to avoid detection or to create a false image that will attract a 'false positive' that could frame innocent users, or flood law enforcement agencies – diverting resources away from real investigations. Other suggested tools are either not effective or make errors.

The next section is 'Technical Implications for Weakening End-to-End Encryption. As they conclude:

> Any law which would mandate CSS, or any other technology designed to access, analyse or share the content of communications will, without a doubt, undermine encryption, and make everyone's communications less safe as a result. The laudable aim of protecting children does not change this technical reality.[16]

[13] See Fts 7-9 for links to the EU, UK and US proposed legislation.

[14] https://edri.org/our-work/open-letter-hundreds-of-scientists-warn-against-eus-proposed-csa-regulation/

[15] Ibid 1

[16] Ibid 3

Finally, they discuss the effectiveness of the Regulation's proposals for addressing the harmful material online. Their conclusion:

> We have serious reservations whether the technologies imposed by the regulation would be effective: perpetrators would be aware of such technologies and would move to new techniques, services and platforms to exchange CSAM information while evading detection. The proposed regulation will harm the freedom of children to express themselves as their conversations could also be triggering alarms. National criminal law enforcement on-the-ground typically deals in a nuanced way with intimate messages between teenagers both around the age of consent. These technologies change the relationship between individuals and their devices, and it will be difficult to reintroduce such nuance. For other users, we have major concerns of the chilling effects created by the presence of these detection mechanisms. Finally, the huge number of false positives that can be expected will require a substantial amount of resources while creating serious risks for all users to be identified incorrectly. These resources would be better spent on other approaches to protect children from sexual abuse.[17]

Impact on Smaller Providers

Both Standards impose a range of activities in the various industry providers. They include as a first step, undertaking a 'risk assessment' based on criteria included in both Standards.[18] They then have to undertake a range of activities that can detect harmful material, as against the service(s) provided.[19] Further, providers of Relevant Electronic Services are required to have a development plan that will further enhance their ability to detect and delete harmful material..[20] There is a similar requirement for Designated Internet Services, but only for those providers with a large amount of active end users.[21]

The Discussion Paper for both Codes also shows concerns for the potential cost burden on smaller providers. In its questions for response, the Paper specifically asks for a response on compliance costs for service providers and, 'in particular, the impact of compliance costs on new entrants.[22]

[17] *bid*

[18] Part 3 in both Standards

[19] Part 4 in both Standards

[20] Standard for Relevant Electronic Services, CL 23

[21] Standard for Designated Internet Services Cl 24

[22] Discussion paper 24, Question 24

A Way Forward

Because of the unclear wording of the "Safety on-line compliance measures' listed in Part 4o of each Standard, it is not clear whether any of those measures amount to interception of communications. We note that law enforcement agencies already have considerable powers to intercept communications within a legal framework. Indeed, although recent amendments to the *Telecommunications Act 1997* gave additional powers to the Attorney-General and the Minister for Communications to jointly issue Technical Assistance Requests (TAR), Technical Assistance Notices(TAN) and Technical Capability Notices (TCN), law enforcement agencies have barely needed these new powers.[23] With apparently more than sufficient powers to access information already legally available to law enforcement agencies, there can be no justification for allowing any interception of communications outside of the existing legal framework.

Internet Australia also supports the open letter to the eSafety Commissioner:

> 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.[24]

The Child Rights International Network suggests ten principles (process and substance) for addressing the issue of online harm, particularly for children.25 These principles provide guidance for a more nuanced approach to the protection of people in an online environment that balances needs for protection and the equally important protections for privacy communications.

Process:

1. Actions affecting the digital environment must respect the full range of children's rights, from protection from violence to privacy and freedom of expression
2. No single law, policy or technology can protect children online or secure their human rights more broadly. Interventions engaging encryption must be seen within a wider ecosystem with many actors

[23] Attorney-General's Department 2021-22, *Annual Report Under the Telecommunications (Interception and Access Act 1979 and Part 15 of the Telecommunications Act 1997.*, p. 2 In the reporting year, there were 30 TAR requests given but no TANs of TCNs were given.

[24] 7 December 2023, signed by the Centre for Democracy and Technology, Global Partners Digital, Internet Freedom Foundation, Internet Society, Access Now, Digital Rights Watch. https://www.globalencryption.org/2023/12/take-action-sign-the-joint-letter-in-response-to-australian-esafety-proposed-industry-standards-2/

[25] CRIN viii-ix

3. All those with relevant expertise (eg in child protection, technology and internet regulation, data protection and privacy, general human rights etc) must be involved in discussions and decision making regarding children and the digital environment including on encryption
4. Children and other directly affected communities, for example survivors of child sexual abuse or those disproportionately affected by intrusive data practices must be heard and their views given due weight
5. The digital environment is interconnected and regulation in one jurisdiction is very likely to cause ripple effects in others. Therefore policy makers engaging with encryption must address the impact beyond their own jurisdiction

Substance

6. There should be no generalised ban on encryption for children
7. Interventions engaging encryption must consider and address specific political, economic and social and cultural contexts
8. Restrictions on qualified children's rights such as privacy must be necessary and proportionate. They should be sufficiently clear and precise, limited to achieving a legitimate goal and the least intrusive in doing so
9. Policy making should address the role of business i
10. Children must have access to justice for all violations of their full range of rights in the digital environment, including where encryption is engaged. Free, effective and child-friendly complaint mechanisms alongside independent oversight mechanisms should be available.

ENDS