December 21, 2023

To: The office of the eSafety Commissioner
Email: submissions@esafety.gov.au

Submission on the draft Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard 2024 and the draft Online Safety (Designated Internet Services – Class 1A and 1B Material) Industry Standard 2024

We thank the office of the eSafety Commissioner for holding this round of consultation on the the Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard 2024 ("Draft RES Standard"), and the draft Online Safety (Designated Internet Services – Class 1A and 1B Material) Industry Standard 2024 ("Draft DIS Standard", collectively "Draft standards").

Access Now is an international non-profit organization which works to defend and extend the digital rights of users at risk globally. Through presence in more than 13 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. Access Now also operates a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We coordinate as part of CiviCERT (Computer Incident Response Center for Civil Society) a Trusted Introducer accredited CERT, and are a member of the global Forum of Incident Response and Security Teams (FiRST). We have special consultative status at the United Nations.[1]

Access Now actively engages with authorities across the world, including in Australia, on protecting human rights in the digital age. We have had opportunities to briefly engage over email with the eSafety Commissioner's office, on behalf of a coalition of stakeholders, in relation to the Draft Standards, and we are grateful for the open channel of communication.

In the past, Access Now has submitted comments on the Draft Online Safety (Basic Online Safety Expectations) Determination 2021, and participated in the virtual consultation

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.

organized by industry associations on the draft industry codes.[2] We made a submission to the steering group of industry associations on the Revised Draft Industry Codes, under the Online Safety Act. Further, we also filed submissions on the reform of Australia's electronic surveillance framework discussion paper[3], and the review of the Privacy Act 1988[4]. Prior to that, we submitted feedback on the Cyber Security Policy Division, Department of Home Affairs, on Australia's 2020 Cyber Security Strategy.[5] Access Now has also provided recommendations on the cyber security infrastructure in Australia through a report titled " Human Rights in the Digital Era: An International Perspective on Australia".[6] We have also participated in the public hearings as well as made written submissions on the implications of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 on human rights, and the changes that are necessary, to the Parliamentary Joint Committee on Intelligence and Security and the Independent National Security Legislation Monitor.[7] Further, we are concerned by the consistent development of an apparatus of surveillance laws in Australia, including through the recently passed Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021.[8]

We write to you to provide our comments based on our expertise working on digital rights in Australia, and across the world.

Feedback on the Draft Standards

We appreciate the eSafety Commissioner's endeavour to enable greater safety online, and to

---

[2] Access Now, *Submission on the Draft Online Safety (Basic Online Safety Expectations) Determination 2021,* https://www.accessnow.org/cms/assets/uploads/2021/11/Australia_Online_Safety_Submission_Nov_2021.pdf

[3] Access Now, *Submission on the Reform of Australia's electronic surveillance framework discussion paper*, https://www.accessnow.org/cms/assets/uploads/2022/02/Australia-Home-Affairs-Department-Surveillance-Review-Access-Now-inputs_February-2022.pdf

[4] Access Now, *Submission on the the Review of the Privacy Act 1988*, https://www.accessnow.org/cms/assets/uploads/2022/01/Australia_Privacy_Act_Submission.pdf

[5] Access Now, *Submission on Australia's 2020 Cyber Security Strategy*, https://www.accessnow.org/cms/assets/uploads/2019/11/Consultation-Australia-2020-cybersecurity-strategy-1-November-2019-.pdf

[6] Access Now, *Human Rights in the Digital Era: An International Perspective on Australia*, https://www.accessnow.org/cms/assets/uploads/2018/07/Human-Rights-in-the-Digital-Era-an-international-perspective-on-Australia.pdf

[7] Access Now, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, https://www.inslm.gov.au/sites/default/files/2019-11/32._access_now.pdf

[8] Access Now, *Surveillance state incoming with Australia's "hacking" bill*, https://www.accessnow.org/surveillance-state-incoming-with-australias-hacking-bill/; Access Now, *To protect human rights, identify and disrupt Australia's "hacking bill"*, https://www.accessnow.org/to-protect-human-rights-identify-and-disrupt-australias-hacking-bill/

make platforms accountable. We also commend the effort put into developing the Draft Standards and the consultations held in that regard.

Our feedback focuses on the impact of the Draft Standards on people's safety and privacy, by virtue of their impact on end-to-end encryption.

The Draft Standards would effectively eradicate end-to-end encryption

We are concerned primarily with Sections 20-23 of the Draft RES Standard and Sections 21-24 of the Draft DIS Standard. These provisions would require a wide category of online communication services, as well as file storage and cloud services, to proactively detect content on their platforms. The Draft Standards seek to impose this mandate on all types of services, without regard to the fundamental difference in their technical capabilities. The inalienable feature of end-to-end encrypted messaging services and cloud storage services is that no third party, not even the service provider itself, can ever access the content that is being exchanged or stored. Encryption therefore empowers people to maintain a level of privacy and security that is otherwise virtually impossible to achieve amid the ceaseless rise in surveillance and cyberattacks.[9]

The Draft Standards require DIS and RES entities to detect and remove known pro-terror material, known child sexual abuse material (CSAM), and to disrupt and deter such types of content. Service providers must implement systems, processes and technologies that detect and identify known CSAM and pro-terror material. Notes in the Draft Standards explain that the systems, processes and technologies that the provider may use include hashing technologies, machine learning and artificial intelligence systems that scan for known CSAM and pro-terror material.

These measures, commonly referred to as "client-side scanning", are effectively a mandate for generalised and bulk surveillance, and therefore violative of human rights. By not exempting encrypted platforms, the Draft Standards will compel such secure channels to fundamentally alter their technological architecture and develop the ability to scan content. **The stage of the communication/storage process at which the content is scanned (eg. before content is uploaded or sent), or the form in which it is scanned (eg. hashes), is immaterial — the introduction of scanning capabilities in any form on encrypted platforms is an erosion of the core privacy and security promise of end-to-end**

[9] Access Now, *Policy Brief: 10 facts to counter encryption myths,* https://www.accessnow.org/wp-content/uploads/2021/08/Encryption-Myths-Facts-Report.pdf

encryption on which people in Australia and across the world rely.

As several security experts, human rights groups, and digital rights advocates have highlighted[10], client-side scanning is not ripe for adoption for a range of reasons, including that (a) scanning mechanisms are deeply flawed and have questionable effectiveness; (b) the risk of false positives is very high; (c) they amplify vulnerabilities to security threats and attack and weaken online safety for all; (d) they can be modified to scan for other types of content, resulting in a chilling effect; (e) tech-solutionism is short-sighted and the solutions to societal problems lie elsewhere through initiatives geared towards social welfare, education etc.; (f) platform accountability is imperative but such measures should focus on user-empowering and rights-respecting mechanisms, unlike client-side scanning; and (g) by their very design, they undermine the privacy and security offered by encryption, which is among the strongest tools we have for online safety today. The need to protect encryption, and the perils of degrading or circumventing it have been set out later in this submission.

For detection and removal of known CSAM and pro-terror content, the Draft Standards state that a service provider will not be required to implement a system, process or technology if it is not technically feasible for the provider to do so. Section 7 sets out that the matters to be considered while determining technical feasibility include "expected financial cost to the provider" and "whether it is reasonable to expect the provider to incur that cost, having regard to the extent of the risk to the online safety of end-users in Australia of not taking the action." **A crucial omission that ought to be rectified is the lack of any mention of the recognised technological inability to implement certain features without fundamentally changing the architecture of the platform by introducing a vulnerability or weakness, such as would be the case if end-to-end encrypted services were to implement scanning and detection mechanisms**.

Another notable discrepancy is that the sections on disruption and deterrence of certain types of content, do not contain a technical feasibility exception, even though they also carry the mandates on scanning and detection that the sections on detection and removal do. This waters down the technical feasibility exception, and creates significant uncertainties for platforms as well as users around implementation. **Platforms could effectively be compelled to introduce the same measures under a different section, even if they are eligible for an exception under other provisions**.

[10] https://www.cl.cam.ac.uk/~rja14/Papers/chatcontrol.pdf ; https://arxiv.org/abs/2110.07450 ; https://www.accessnow.org/press-release/apple-encryption-expanded-protections-children/

The eSafety Commissioner has made public statements in support of privacy and security, and provided reassurances noting that the regulation would not require building weakness or undermining end-to-end encryption. However, we respectfully submit that the mandate for proactive detection and scanning in the Draft Standards run counter to this position, as they would create a vulnerability in the system and undermine encryption. We urge the eSafety commissioner to amend the Draft Standards to reflect the stated commitment to strengthening privacy and security, and better protect the enabling tool, i.e. end-to-end encryption .

We acknowledge the severity of harm caused by the dissemination of CSAM and other types of illegal content, and support the endeavour to regulate platforms to ensure accountability and empowerment of all users to enable them to exercise fundamental rights and remain safe. However, in weakening the security and privacy promise of encryption, the Draft Standards will not only fail to achieve this goal, but will also aggravate existing safety challenges by creating greater vulnerability and insecurity.

End-to-end encryption is vital for everyone's safety

As privacy and cybersecurity expert Susan Landau put it, "In a world in which securing communication bits is equivalent to securing money, ideas, and business and personal information, end-to-end encryption is integral to public safety and national security."[11]

End-to-end encryption is among the most powerful defences we have against the plethora of threats online to both data in transit, over messaging platforms for instance, and data in storage, for example, in the cloud. The scale of personal data of each individual that is available in the digital domain, both through voluntary actions, and through scraping, aggregation and inferences by service providers, often unknown to the data subject, is unprecedented and unfathomable. Equally hard to imagine, is the vulnerability of such personal data. Rapid digitisation is coupled with increasing threat vectors online, with attackers becoming increasingly sophisticated at circumventing safeguards and exploiting personal information.

Cyberattacks and data breaches are on the rise across the world and Australia is no exception. Australia is among the top four most targeted countries in the world by cybercriminals, along

[11] Lawfare, *How the U.K. and the Senate Judiciary Committee Are Being Dangerously Foolish About Cryptography*, https://www.lawfaremedia.org/article/how-uk-and-senate-judiciary-committee-are-being-dangerously-foolish-about-cryptography

with the UK, the US and Canada.[12] In Australia, Canada and the UK, the number of accounts breached in the first half of 2023 was more than double the number of accounts breached in the first half of 2022. The Australian Cyber Security Centre noted a 23% increase in cybercrime reports in the 2023 fiscal year as compared to the previous year.[13]

The victims of cyberattacks include the more vulnerable groups of society. Schools, for instance, are a top target for ransomware and other types of cyberattacks. A survey spanning 14 countries and 3000 IT professionals found that 80% of education providers reported that they were hit by ransomware.[14] Earlier this year, a school in the US reported that a breach had resulted in the exposure of over 300,000 highly sensitive files of students' data, including information about sexual assaults, psychiatric hospitalizations, abusive parents, and suicide attempts.[15] Over this year, there have been several other instances of students' and children's sensitive data, including names, addresses, financial information, and health information being compromised, impacting millions.[16]

End-to-end encryption is the most secure technology we have today to safeguard personal data, and can help prevent attacks and breaches, by making it virtually impossible for hackers to misuse personal data. Ivan Krstić, head of Apple Security Engineering and Architecture (SEAR), believes that "[i]t is conceivable in theory to attempt to break the encryption by trying every possible key, but we can quantify how long this would take: The attacker has virtually no chance of success before our sun runs out of hydrogen, sputters, and extinguishes."[17] End-to-end encryption therefore enhances online safety for all, by providing secure channels

---

[12] Professor Stuart E. Madnick, Ph.D, *The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase*, https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf

[13] Australian Signals Directorate, *ASD Cyber Threat Report 2022-2023,* https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

[14] Sophos, *The State of Ransomware in Education 2023,* https://assets.sophos.com/X24WTUEQ/at/j74v496cfwh4qsvgqhs4pmw/sophos-state-of-ransomware-education-2023-wp.pdf

[15] AP News, *Ransomware criminals are dumping kids' private files online after school hacks*, https://apnews.com/article/schools-ransomware-data-breach-40ebeda010158f04a1ef14607bfed9b0

[16] The Guardian, *Tasmanian data breach: schoolchildren's information among 16,000 documents leaked on dark web*, https://www.theguardian.com/australia-news/2023/apr/07/tasmanian-data-breach-schoolchildrens-information-among-16000-documents-leaked-on-dark-web ; *Bleeping Computer, SickKids impacted by BORN Ontario data breach that hit 3.4 million*, https://www.bleepingcomputer.com/news/security/sickkids-impacted-by-born-ontario-data-breach-that-hit-34-million/

[17] Lawfare, *Personal Data in the Cloud Is Under Siege. End-to-End Encryption Is Our Most Powerful Defense*, https://www.lawfaremedia.org/article/personal-data-in-the-cloud-is-under-siege.-end-to-end-encryption-is-our-most-powerful-defense

for communication, transfer and storage of files. Undermining this critical tool would cause grave harm to security, not only online but also offline, given how intertwined the two spaces have now become.

A report by two children's rights organizations, the Child Rights International Network (CRIN) and Defend Digital Me (DDM), shows how encryption contributes to the protection of children, especially the most vulnerable among them.[18] It includes a recommendation that encryption not be banned from the services that children use and a recommendation that measures engaging encryption must meet the international law standard of being necessary and proportionate.

The role of encryption in protecting children has also been recognised by researchers associated with UNICEF, in a working paper titled "Encryption, Privacy and Children's Right to Protection from Harm".[19] Some of the particularly pertinent observations, which were also highlighted by Riana Pfefferkorn, Research Scholar at the Internet Observatory at Stanford University, in her letter[20] to the European Commission on the proposed CSA, are reproduced below:

- "End-to-end encryption is necessary to protect the privacy and security of all people using digital communications channels. This includes children…" (p. 3 of the working paper)
- "[T]he goal of ensuring that children's rights are safeguarded in the digital age involves fulfilment of their rights to both privacy and protection from sexual abuse and exploitation. Privacy is often treated as a secondary right. Thus, debates around end-to-end encryption have tended to assume that a safety-maximizing solution (or even a privacy-minimizing solution) is the best way to keep children safe, which is not always the case." (p. 5)
- "[E]ncryption is fundamental for any democratic and rights-respecting state to protect its citizens, including children who are increasingly gaining access to digital communications platforms." (p. 6)

---

[18] Child Rights International Network, *Privacy and Protection: A children's rights approach to encryption*, https://home.crin.org/readlistenwatch/stories/privacy-and-protection

[19] UNICEF, Encryption, *Privacy and Children's Right to Protection from Harm*, https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf

[20] Riana Pfefferkorn, *Feedback on the European Commission's proposed regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 2022/0155 (COD)*, https://cyberlaw.stanford.edu/sites/default/files/publication/files/2022-05-18%20Letter%20to%20EU%20Comm%27n%20re%20CSA%20scanning%20draft%20reg.pdf

- "Encryption is also critical to ensure children's safety." (p. 6)
- "Children have a right to be protected from sexual abuse and exploitation wherever it occurs, including online … At the same time, end-to-end encryption by default on … digital communication platforms means that every single person, whether child or adult, will be provided with a technological shield against violations of their right to privacy and freedom of expression." (p. 8)
- "In the end, we need to appreciate that the right to protection includes ensuring privacy and security." (p. 13)
- "[I]t is incorrect to suggest that children will have their rights better respected if digital communications platforms remain unencrypted…" (p. 13)
- "Certainly, violations of a child's right to protection from sexual abuse and exploitation have severe and often lifelong consequences. For some, the consequences of privacy, security and data protection risks can also be severe, long-term." (p. 13)

The UNICEF paper also recognizes the complexity and difficulty of policy development to protect children in the age of the internet without unnecessarily undermining other co-equal rights including the right to privacy. We acknowledge the extremely difficult task before the eSafety Commission to balance these rights. However, **the mandates in the Draft Standards fail to strike this balance, and will do more harm than good by eroding end-to-end encryption, and therefore privacy and security**.

A more holistic assessment of the impact on the full scale of the people's rights, including of course those who are most vulnerable online (and offline), is essential to arrive at an effective solution and this would not entail weakening encryption.

Undermining encryption would imperil fundamental rights and harm the economy

With the increase in overt and covert forms of surveillance from state and non-state actors, including large scale deployment of spyware[21] and other types of surveillance technology, enabling tools for online security such as encryption have become more important than ever.

Encrypted platforms allow people to communicate and exchange information freely without fear of prying eyes, and therefore protect the human rights to privacy, free expression, information and assembly. Encryption makes it possible for students to receive online education without the confidentiality and authenticity of the channel and participants being compromised; for a journalist to protect the identity of their source; for individuals to safely

[21]The Guardian, *The Pegasus Project*, https://www.theguardian.com/news/series/pegasus-project

share sensitive health information and receive healthcare, including pregnant women, and parents who may need to do so for their children; for businesses to share trade secrets; and for human rights defenders to share potentially life-threatening information without fear of surveillance and persecution. While the unavailability of secure channels violates the fundamental rights of all, certain sections of society, including journalists, human rights defenders, activists, and others, are disproportionately impacted.

As the American Civil Liberties Union puts it, "[i]t is nearly impossible to quantify the fallout from the persecution of people betrayed by insecure messaging, whether it be an increase in domestic violence, a chilling effect on journalists and whistleblowers, the concentration of power in the hands of corporate and government elites, the silencing of dissent, or the neutralising of political opposition."[22]

Any policy that weakens the privacy assured by encryption, as the Draft Standards do, sets a very dangerous precedent, and the global ramifications ought to be considered. A proactive monitoring and detection ability is essentially a vulnerability or a weakness on an encrypted platform. Once it has been introduced, it makes the platform and all its users vulnerable to attack. There is no sure way to ensure that (a) only the authorised agencies can access the content, while keeping malicious actors at bay; and (b) the scanning mechanism is used only for certain types of content.

With respect to (a), it must be noted that the scanning mandate in the Draft Standards will not only weaken privacy in Australia, but also worldwide, especially for those who communicate and transact with people in Australia – they will be compelled to resort to compromised platforms. The threat to encryption, a crucial tool for cyber resilience, will also consequently stifle innovation in the cybersecurity space in Australia, putting Australian individuals and companies on the backfoot as compared to their foreign counterparts. In the past, laws threatening encryption have already compelled certain tech platforms to retreat from Australia.[23] In an Australia-focused study titled "The Economic Impact of Laws that Weaken Encryption", the Internet Society found that encryption-weakening frameworks – which we believe the Draft Standards are – increase business uncertainty, undermine the brand image of service providers with operations in Australia and therefore vulnerability to the threats of the laws there, and reduce trust in digital services, ultimately having an adverse impact on the

[22] American Civil Liberties Union, *The Vital Role of End-to-End Encryption*, https://www.aclu.org/news/privacy-technology/the-vital-role-of-end-to-end-encryption
[23] ZD Net, *Encryption laws are creating an exodus of data from Australia: Vault*, https://www.zdnet.com/article/encryption-laws-are-creating-an-exodus-of-data-from-australia-vault/

economy.[24]

On (b), the domino effect of one country, particularly a modern democracy, introducing scanning requirements, cannot be overemphasised. It is only a matter of time before scope creep kicks in and authoritarian governments impose mandates to expand the scope of proactive monitoring and detection on encrypted platforms. Once the technology is created and made available – it will be misused for all types of content that a particular government may find unfavourable. The chilling effect on free speech will quell political and artistic material, and disproportionately impact vulnerable communities. WeChat[25] in China is an example of how authoritarian regimes can weaponize private messaging platforms for surveillance and censorship.

Weakening encryption is a disproportionate measure and will not achieve the stated goals, doing more harm than good

As stated before, the intention to make the internet safer is one that resonates with all stakeholders. We are cognizant of the urgent need to address the issue, and support efforts to work with all stakeholders involved to arrive at rights-respecting solutions. However, a mandate for generalised surveillance, as set out in the Draft Standards by requiring proactive scanning/detection of content, would only serve to treat every single person who uses an platform as a suspect – stifling their ability to express themselves – and make the internet vulnerable and less secure, including for the very people the eSafety Commission seeks to protect. As the European Court of Human Rights has observed[26], the mere existence of a law authorizing secret monitoring of communications is at odds with the freedom of expression and the right to privacy.

Scanning mechanisms on encrypted platforms of the sort contained in the Draft Standards amount to indiscriminate surveillance, are inherently disproportionate and unjustifiable given the direct impact on the human rights to privacy and free expression.

---

[24] Internet Society, *New Study Finds Australia's TOLA Law Poses Long-Term Risks to Australian Economy*, https://www.internetsociety.org/news/press-releases/2021/new-study-finds-australias-tola-law-poses-long-term-risks-to-australian-economy/

[25] The Citizen Lab, *We Chat, They Watch*, https://citizenlab.ca/2020/05/we-chat-they-watch/

[26] Report of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age*, August 2018, https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.docx ; European Court of Human Rights, Roman Zakharov v. Russia, application No. 47143/06, judgement of 4 December 2015.

A public petition[27] opposing the CSA Regulation in the EU, which mandates scanning as the Draft Standards do, highlights that "[t]he United Nations and UNICEF state, online privacy is vital for young people's development and self-expression, and children should not be subjected to generalised surveillance. The UK Royal College of Psychiatrists highlights that snooping is harmful for children, and that policies based on empowerment and education are more effective…. [The] proposal would also harm whistleblowers, activists in political opposition, labour unions, people seeking abortions in places where it is criminalised, media freedom, marginalised groups and many others. This will set a dangerous precedent for mass surveillance around the world." The petition was signed by over 2,00,000 people and 133 NGOs. The European Parliament has rejected scanning of huge volumes of private data as would be required by the proposed CSA regulation.[28]

The human rights harms of weakening or circumventing end-to-end encryption are clear. However, the stated benefits of doing so remain hypothetical. For instance, if scanning capabilities are introduced, bad actors will merely shift to other encrypted platforms available in other jurisdictions or in the black market, or create their own, in order to conceal their activities. The problem would then persist, but move out of law enforcement's reach, precluding lawful assistance from platforms and access even to metadata – which to be clear, can often be more sensitive than the content of messages itself[29], and must only be permitted in a manner that is necessary and proportionate – which can be instrumental in investigations.

In any case, even if scanning were to hypothetically increase the probability of prosecution, it simply fails to fulfil the tests of necessity and proportionality that are essential for any impingement on fundamental human rights, including privacy and free expression. Even in the offline world, there are several measures that, when considered in isolation devoid of the impact on rights, could make investigations by law enforcement and government agencies easier. However, limitations exist precisely because permitting certain measures would be unnecessary, disproportionate and violative of fundamental rights.

Further, research also demonstrates that rights-respecting, content-oblivious and effective

[27]Stop Scanning Me, https://stopscanningme.eu/en/
[28] European Digital Rights (EDRi), *CSAR: European Parliament rejects mass scanning of private messages. Here is why*, https://edri.org/our-work/csar-european-parliament-rejects-mass-scanning-of-private-messages/
[29] Just Security, *Michael Hayden: "We Kill People Based on Metadata"*, https://www.justsecurity.org/10311/michael-hayden-kill-people-based-metadata/

solutions exist, and can be developed, to combat the spread of illegal content, including metadata analysis, user education, improved design to encourage reporting, and consistency of enforcement decisions.[30]

Research scholar Riana Pfefferkorn surveyed a group of online service providers serving over 2 billion users about the "trust and safety" techniques they employ to detect, prevent, and mitigate abuse on their services. She found that automated scanning is not the only, or best, way to detect grooming. Pfefferkorn states: "It is urgent that regulators understand the shortcomings of automated abuse detection … Irrespective of their dubious legality, [my] results indicate that … automated scanning mandates may not fix the problems that governments intend them to solve. … [G]overnments seeking to reduce the online prevalence of [CSA and other abuse] (without degrading the rights of their citizens) should start by incentivizing more providers to implement strong reporting tools before requiring [automated content scanning]."[31]

Encryption is vital for privacy and the threat to it in the Draft Standards contravenes the privacy reforms underway in Australia

We also urge whole-of-government consistency in approaching this subject. The Australian government is taking commendable steps to reform laws governing electronic surveillance and privacy. The Attorney-General's Department's objectives for the electronic surveillance reform state that the revised laws will "protect privacy; promote transparency; and be explicit for agencies, oversight bodies, industry and the public."[32] With reference to the ongoing review of the Privacy Act, the AG's Department notes that "reforms are aimed at strengthening the protection of personal information and the control individuals have over their information. Stronger privacy protections would support digital innovation and enhance

---

[30] Riana Pfefferkorn, *Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3920031; Center for Democracy & Technology, *Outside Looking In: Approaches to Content Moderation in End-to-End Encrypted Systems*, https://cdt.org/insights/outside-looking-in-approaches-to-content-moderation-in-end-to-end-encrypted-systems/

[31] Riana Pfefferkorn, *Feedback on the European Commission's proposed regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 2022/0155 (COD),* https://cyberlaw.stanford.edu/sites/default/files/publication/files/2022-05-18%20Letter%20to%20EU%20Comm%27n%20re%20CSA%20scanning%20draft%20reg.pdf

[32] Australian Government, Attorney General's Department, *Reform of Australia's electronic surveillance framework*, https://www.ag.gov.au/crime/telecommunications-interception-and-surveillance/reform-australias-electronic-surveillance-framework

Australia's reputation as a trusted trading partner."[33]

As submitted in a joint letter supported by 30 signatories[34], the threat to encryption in the form of proactive detection mandates in the Draft Standards is at odds with the ongoing privacy and electronic surveillance reform in Australia, and categorical protection of end-to-end encryption "is essential to achieve the goals underlying the Australian government's wider efforts to reform surveillance and privacy frameworks, and protect online privacy and security".

Access now recommends:

- Elimination of the mandate to proactively and indiscriminately detect, monitor, and scan content as it amounts to generalised bulk surveillance that is incompatible with human rights;
- Incorporating a categorical exemption for encrypted platforms from having to comply with detection or scanning requirements. As set out in this submission, encryption is crucial for privacy and security, and to strengthen human rights in the digital age, and scanning mandates would necessarily undermine this critical technology and the rights it protects, while making the internet more unsafe for all;
- That the section on technical feasibility be amended to recognise the technological inability to implement certain features, without fundamentally changing the architecture of the platform by introducing a vulnerability or weakness, such as would be the case if end-to-end encrypted services were to implement scanning and detection mechanisms.
- The technical feasibility exemption, with the section on technical feasibility amended as recommended above, must also apply to the mandate to disrupt and deter content, and any other provision that would require platforms to develop new technical capabilities, as it does to the mandate to detect and remove content.
- Incorporating categorical protection for end-to-end encryption to ensure meaningful alignment with the Australian government's efforts to reform the privacy and surveillance framework and furthering Australia's efforts on global privacy leadership.

[33] Australian Government, Attorney General's Department, *Privacy Act Review Report*, https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

[34] Access Now, *Joint letter: the Australian government must incorporate safeguards for encryption in the online safety codes*, https://www.accessnow.org/press-release/joint-letter-australia-encryption-online-safety-codes/

Conclusion

Thank you for the opportunity to participate in this consultation. We remain available for any clarification or queries in relation to this feedback, and hope to be of further assistance in this important process.

Yours sincerely,

Namrata Maheshwari
Asia Pacific Policy Counsel
namrata@accessnow.org

Raman Jit Singh Chima
Asia Pacific Policy Director
raman@accessnow.org

Access Now | https://www.accessnow.org