23 March 2023

To:
The steering group of industry associations:

BSA | the Software Alliance (BSA),
the Australian Mobile Telecommunications Association (AMTA),
Communications Alliance,
the Consumer Electronics Suppliers Association (CESA),
the Digital Industry Group Inc (DIGI), and
the Interactive Games and Entertainment Association (IGEA).

Email: hello@onlinesafety.org.au

Submission on the Revised Draft Industry Codes, under the Online Safety Act

We thank the industry associations for holding this round of consultation on the revised Draft Industry Codes ("Draft Codes").

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 had submitted comments on the Draft Online Safety (Basic Online Safety Expectations) Determination 2021, and participated in the virtual consultation organized by industry associations on the draft industry codes.[2] We also filed submissions on the reform of

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

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.

The Revised Draft Industry Codes

We appreciate the Australian government's effort to enable greater transparency and accountability of social media services, electronic services and designated internet services, and to ensure online safety for end-users. We also commend the effort put in by industry associations into developing the Draft Codes and the consultations held in that regard.

At the outset, we submit that any legislative or regulatory instrument that seeks to govern the experience of users online, as the Draft Codes do, has a direct impact on people's rights and freedoms. The central focus of such a legislative instrument should be strengthening users' rights and safety, and therefore any provision that compromises this goal must be amended or eliminated.

---

[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/

Our comments in this submission are tailored to certain sections of the Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms; Schedule 2 – Relevant Electronic Services Online Safety Code (Class 1A and Class 1B Material); and Schedule 3 – Designated Internet Services Online Safety Code (Class 1A and Class 1B Material), that impact encryption, and consequently people's privacy, security and free expression.

Encryption enables online safety for all

As the government and industry associations devise policies to govern online content and ensure safety, we submit the following broader comments on the role that encryption plays in protecting human rights.

Strong encryption[9], including end-to-end encryption, is essential for protecting privacy, free expression, and other human rights. **Encryption contributes to the online safety of all, including children by ensuring that only the sender and intended recipient/s can access the information exchanged, preventing access by any third party, including the service provider itself, preserving the integrity of information and allowing for authentication of identities**.

The "privacy versus safety" debate rests on a false binary. These two are mutually reinforcing ideals, and weakening one necessarily weakens the other. Any measures that weaken, undermine or circumvent encryption, have a debilitating effect on privacy as well as security for each individual. A policy that aims to strengthen online safety, without adequately protecting and strengthening encryption, does more harm than good and will result in more insecurity than security.

The critical role of encryption as an enabler of privacy and human rights has been widely recognized, including by United Nations agencies. Last year, the Report of the Office of the United Nations High Commissioner for Human Rights on The Right to Privacy in the Digital Age, noted "Encryption is a key enabler of privacy and security online and is essential for safeguarding rights, including the rights to freedom of opinion and expression, freedom of association and peaceful assembly, security, health and non-discrimination. Encryption ensures that people can share information freely, without fear that their information may become known to others, be they State authorities or cybercriminals[…]In recent years, various Governments have taken actions, which, intentionally or not, risk undermining the security and confidentiality of encrypted communications. This has concerning implications for the enjoyment of the right to privacy and other human rights."[10]

[9] By "strong encryption" we mean encryption that is not broken, weakened, undermined, or circumvented, including through any backdoors, exceptional access mechanisms, or other measures, that would enable access to encrypted data by any entity other than the authorized parties.
[10] Human Rights Council, *Report of the Office of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age*, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement

UNICEF also recognizes the role that encryption plays in protecting children's fundamental rights. As researcher Riana Pfefferkorn states in her feedback on one set of proposed rules in the Europe Union to monitor communications, including on encrypted platforms, to combat child sexual abuse: "In an October 2020 working paper titled Encryption, Privacy and Children's Right to Protection from Harm, UNICEF's Office of Research - Innocenti emphasized the importance of including children's privacy rights in policy discussions about child safety. It cautioned states against enacting policies undermining encryption in the name of protecting children, given the vital role that encryption plays in protecting children's privacy, security, and safety."[11]

Further, a recent report from two children's rights organizations, the Child Rights International Network and Defend Digital Me, highlights that encryption protects children, especially the most vulnerable among them. The report recommends that encryption not be banned from the services that children use, and that measures involving encryption must meet the international law standard of necessity and proportionality.[12]

When encryption is weakened through mandates such as those requiring service providers to scan content, it jeopardizes people's ability to express themselves freely and communicate safely, with a disproportionate impact on the most at-risk individuals and organizations in our communities.[13] Even if the policy mandate is to implement such measures only for a select set of illegal materials, this is not technically possible. Once the ability to scan is created, or otherwise weaken or circumvent end-to-end encryption, the security tool no longer exists in the form that is essential for privacy and safety. It is then a vulnerability, jeopardizing privacy and free speech online, susceptible to being exploited by malicious state and non-state actors.

Further, such policies set a dangerous precedent. As a result of scope creep, there is the looming threat of authoritarian regimes - citing Australia's example - to push technology platforms to expand the mandate to require scanning of all types of material, including dissent, resulting in a chilling effect on free speech, and expansive surveillance that damages human rights across geographies. With the continuing increase in surveillance from the private and public sector, and rise in the threat of spyware and other surveillance technologies, privacy and security-preserving tools such as encryption are in greater need of strengthening than ever before.

Access Now recommends that any policy measures, whether framed by the government or industry,

---

[11] 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

[12] https://home.crin.org/readlistenwatch/stories/privacy-and-protection

[13] Access Now, *Who we hurt when we attack encryption*, https://www.accessnow.org/who-we-hurt-when-we-attack-encryption/

that would require encryption to be weakened, undermined or circumvented, must be viewed as antithetical to human rights and online safety, and must not be implemented, as encryption is essential for the privacy and safety of online spaces, and plays a crucial role in protecting human rights.

Encryption and the Draft Codes

Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms

I. We appreciate the language in Clause 6.1 which notes that Code does not require industry to take steps that could "implement or build a systematic weakness, or a systematic vulnerability, into a form of encrypted service or other information security measure; (b) build a new decryption capability in relation to encrypted services; (c) render methods of encryption less effective; (d) undertake monitoring of private communications between end-users." However, we believe that for the intent to be achieved, further changes are necessary.

Access Now recommends modifying clause 6.1(c) to: **"**render methods of encryption *or other information security measures* less effective". It is important to include "*other information security measures*" – which was part of the earlier draft – as technologies are constantly evolving, and this is necessary for the code to remain sustainable and relevant over time and through innovations, while remaining committed to the underlying principle. This limitation must extend to all industry participants and service providers impacted by the Codes and corresponding Schedules.

II. The note following Clause 6.1(d) states that "In considering whether it would be reasonable for an industry participant to adopt a particular compliance measure under this Code, it will be relevant for the industry participant to take into account the desirability of not intruding upon, and otherwise maintaining the privacy and integrity of, private communications between end-users. However, where indicated in the Schedule, *it may be appropriate for an industry participant to adopt measures that involve analysis of behavioural signals and other data or trends in order to prevent, detect and address harmful activity*."

This note appears to refer to the use of metadata and other information available to service providers, other than the content of messages on end-to-end encrypted platforms – eg. profile picture, who sent a message to whom and when etc. We submit that certain end-to-end encrypted platforms refrain from collecting such data about their users, in order to provide a higher level of privacy and security, and they must be allowed to thrive. There are situations where metadata could prove to be even more sensitive than the content of communications.

For example, just the fact of whether and when an individual A messaged individual B, can prove to be valuable information for the government or malicious actor – especially in the case of whistleblowers or journalist's sources. As such, the collection of metadata should never be mandated, and must be permissible only within the bounds of a legal framework that protects human rights and prescribes stringent standards of necessity and proportionality.

Access Now recommends the removal of the following text: **"**However, where indicated in the Schedule, it may be appropriate for an industry participant to adopt measures that involve analysis of behavioural signals and other data or trends in order to prevent, detect and address harmful activity." The data covered by this language can be deeply sensitive, and crucial to preserving the right to privacy and freedom of expression. Platforms committed to maintaining the privacy and integrity of private communications between end-users should not be placed under any obligation, whether direct or indirect, to redesign their functions to collect or analyze metadata in a manner not aligned with necessity and proportionality. Even if the language is retained, it must be clarified that such collection and analysis of metadata is purely voluntary, and platforms will not be required to develop new capabilities to collect more of people's data as that would not be necessary and proportionate.

III. The language in the Code that aims to protect encrypted communication platforms from having to monitor content is severely diluted by Clause 6.2. Clause 6.2 states that an industry participant would not be in violation of the Code if it takes action required under another Australian law. The current legal and regulatory framework in Australia imperils end-to-end encryption, particularly through the Telecommunications and Other Legislation Amendment Act, and the Identify and Disrupt Act, for instance. These laws confer expansive surveillance and interception powers on government and law enforcement agencies, including in respect of encrypted platforms.

Access Now recommends that in addition to committing to voluntarily protecting and strengthening encryption, industry associations must also commit to pushing back against other Australian laws that undermine encryption, including publishing further information on the harms caused by the present legal framework - whose reform is still pending even after the recommendations of the Independent National Security Law Legislation Monitor (INSLM) in July 2020.[14] "An industry participant will not be in breach of this Code merely where it takes an action in Australia that is required by another Australian law or regulation by which the industry participant is bound, *provided it is consistent with necessity and proportionality standards, and the industry participant's responsibilities under the UN Guiding Principles of Business and Human Rights*."

[14] Access Now, Access Now welcomes INSLM recommendations on TOLA reform, https://www.accessnow.org/press-release/access-now-welcomes-inslm-recommendations-on-tola-reform/.

Schedule 2 – Relevant Electronic Services Online Safety Code (Class 1A and Class 1B Material)

IV. We appreciate the inclusion of language meant to ensure that the compliance measures for encrypted services are premised on the actual capability of service providers to review or remove material on their services. The clarification in certain compliance measures, noting that they would not require service providers to conduct client-side scanning, prevent services from adopting encryption or require them to break or weaken encryption, is welcome. However, we believe that certain modifications are necessary to further strengthen encryption and prevent ambiguity.

Access Now recommends amending the language to prohibit any requirement to "*undertake any other measure that may weaken or circumvent encryption*" alongside client side scanning, in order to strengthen protection for encryption, and to avoid any potential ambiguity. Further, the language set out above, with the recommended modification, should be incorporated into a separate overarching clause in the Codes as applicable to all services providing encryption in transit and at rest, in respect of all compliance measures, instead of as a note to specific compliance measures as in.

V. Compliance measure 10 states that encrypted services must "invest in systems, processes, and/or technologies that aim to disrupt and/or deter end-users from using the service to create, post or disseminate CSAM and pro-terror material." Further, the guidance in respect of this measure notes that "[i]n implementing this measure, providers must consider that the threat to online safety posed by new CSAM and pro-terror materials is often different to the threat posed by known materials. Newly generated material is more likely to indicate current and ongoing safety risks such as against a child being groomed and coerced into producing new abusive images".

We are concerned that the above language does not place adequate limitations on the types of systems, processes, or technologies that encrypted services may be compelled to invest in. Most of the proposals to curb the spread of CSAM and promotion of terrorism materials entail content monitoring measures that undermine end-to-end encryption. The particular reference to newly generated material in the guidance note amplifies the concern that encrypted services might be forced to indulge in some form of proactive content monitoring, thereby compelling them to fundamentally alter their architecture in a manner that undercuts privacy and security.

Access Now recommends including a categorical clarification, in compliance measure 10, as well as the Codes more broadly, stating that encrypted services would not, for any purpose, be

required to develop content monitoring mechanisms, or any other measures, that would weaken or circumvent end-to-end encryption.

VI. Compliance measure 17, on "updates and consultation with eSafety about relevant changes to technology", requires encrypted services to "share information with eSafety about significant new features or functions released by the provider of the relevant electronic service that the provider reasonably considers are likely to have a significant effect on the access or exposure to, distribution of, and online storage of class 1A or class 1B materials…".

This measure lacks clarity. In order to avoid over-reporting, under-reporting, or inaccurate reporting, there is a need for explanation on what the threshold for assessing "significance" would be in terms of the nature of the new feature, or the effect on access, exposure, distribution and storage in respect of class 1A or class 1B materials. Further, given the mention of "consultation" in the title of the measure, but lack of explanation thereafter, it is not clear if services would be required to consult with esafety regarding new features or functions, with the rollout being contingent on the outcome. Without greater clarity and limitations, this measure may lead to friction in the implementation of privacy-preserving features.

Access Now recommends amending compliance measure 17 to provide clarity on the factors for assessing "significance" and safeguards to ensure that each new feature on encrypted platforms, including those intended for enhanced privacy and security, does not have to go through a consultation or approval process.

Schedule 3 – Designated Internet Services Online Safety Code (Class 1A and Class 1B Material)

VII. "Designated Internet Services" have an extremely broad definition under the Code and include a vast range of diverse services, such as grocery and retail websites, apps offered by medical providers, news platforms, blogs and encrypted cloud storage services.

The core architecture of the services covered by this definition, and their primary functions, differ considerably. An attempt to govern each of these services, despite the creation of tiers of risk profiles, fails to take into account unique aspects of each service based on its size, functionality, and the ultimate effect of compliance measures on users of specific services. This will also inevitably result in ambiguity.

Access Now recommends narrowing down the definition of designated internet services, creating further categorisations in consultation with stakeholders, and devising separate compliance measures for them that take into account the size, scale, architecture, and

functionality of the service, and the effect of each compliance measure on the end-user.

VIII. We appreciate the recognition that certain end-user managed hosting services, such as those that provide encryption, are not capable of assessing or reviewing materials uploaded by users, or end-user activity, and therefore cannot proactively assess breaches.

Encrypted cloud storage services play a crucial role in ensuring that people's personal data –much of which is housed online in today's day and age – remains safe from unwarranted access and surveillance. As in the case of encrypted communication channels, a defining characteristic of such services is that no third party can gain access to the content, not even the service provider itself.

Designated internet services that do have the capability of viewing content or end-user activity, have an obligation under the code to provide a "variety of potential enforcement measures". The scope of such measures is not clear, and clear limitations are necessary to safeguard encryption.

Access Now recommends incorporating a clarification and safeguard noting that the obligation to provide "potential enforcement measures" would not in any circumstances include measures that directly or indirectly undermine encryption.

IX. The Code prescribes compliance measures to achieve the goal of safety by design. This includes using "the safety by design tools published by eSafety to assess the safety risks associated with a new feature." As set out above, privacy and safety are often presented as a false binary, and privacy-enhancing features are characterized by some as safety-reducing features.

We submit that privacy by design is an important component of ensuring safety, and must equally be built into the code alongside safety by design. The Code must clarify that new features, including those that entail enhanced data protection, privacy and security, would not be subject to limitations and approval processes, on the ground that they negatively impact risk assessment and perceptions of online safety.

Access Now recommends that the Code be amended to require privacy by design alongside safety by design, as privacy is an inalienable component of online safety. Further, it must be clarified that assessments pertaining to new features, including those enabling enhanced data protection, privacy and security, would not be subject to limitations and approval processes, on the ground that they negatively impact risk assessment and perceptions of online safety.

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, Access Now
namrata@accessnow.org

Raman Jit Singh Chima
Senior International Counsel and Asia Pacific Policy Director, Access Now
raman@accessnow.org

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