12 November 2021

To:
Director, Online Safety Reform and Research Section
Department of Infrastructure, Transport, Regional Development and Communications
[redacted]
[redacted]
Email: OnlineSafety@infrastructure.gov.au

Submission on the Draft Online Safety (Basic Online Safety Expectations) Determination 2021

We thank the Australian Department of Infrastructure, Transport, Regional Development and Communications for holding this round of consultation on the Draft Online Safety (Basic Online Safety Expectations) Determination 2021 ("Draft BOSE").

Access Now is an international non profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence in 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 engages with its global community of nearly half a million users from over 185 countries, in addition to operating 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.

Access Now actively engages with authorities across the world, including in Australia, on protecting human rights in the digital age. We had submitted comments to the Cyber Security Policy Division, Department of Home Affairs, on Australia's 2020 Cyber Security Strategy.[2] Access Now has also provided recommendations on the cyber security infrastructure in Australia through

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.
[2] 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

a report titled " Human Rights in the Digital Era: An International Perspective on Australia".[3] 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.[4] 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.[5]

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

The Draft Online Safety (Basic Online Safety Expectations) Determination 2021

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. Any legislative instrument that seeks to regulate the experience of users online, as the Draft BOSE does, has a direct impact on people's rights and freedoms. Therefore, the central focus of such a legislative instrument should be strengthening users' rights and safety, and any provision that compromises this goal must be amended or eliminated.

While certain proposed provisions in the Draft BOSE regarding the creation of effective reporting mechanisms are aligned with this goal, we are concerned that certain other provisions will have the contrary effect of undermining users' safety and jeopardizing their right to privacy and freedom of expression, while amplifying the scope for unwarranted surveillance.

Section 8 threatens encryption which is crucial for online safety:

Strong encryption[6], including end to end encryption, is essential for protecting privacy, free

[3] 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

[4] 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

[5] 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/

[6] 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.

expression, and other human rights, and also for bulwarking the economy, preserving democratic processes and participation, as well as ensuring national security.[7] Section 8 of the Draft BOSE will undermine encryption and imperil each of these defining elements of a free and open society.

Encryption is vital for the protection of the right to privacy[8] and the right to freedom of opinion and expression[9] in the digital age. Therefore, any restriction on encryption must adhere to strict standards of necessity and proportionality. [0] **Section 8 of the Draft BOSE unfortunately fails to meet this threshold**.

Section 8 of the Draft BOSE states: "If the service uses encryption, the provider of the service will take reasonable steps to develop and implement processes to detect and address material or activity on the service that is or may be unlawful or harmful."

This Section is not consistent with the way encryption, particularly end to end encryption, works. It makes the flawed assumption that end to end encrypted communications service providers are in a position to develop technical capabilities to *detect and address* content, without any action from the users. In other words, it is based on the incorrect premise that platforms can be end to end encrypted even if mechanisms are built in to detect and address content, without proactive action from the users. This is paradoxical.

A defining characteristic of end to end encrypted platforms is that only the sender and the intended recipient/s have access to the content that has been exchanged. No third party, including the service provider itself, can gain access to such content. Section 8 ignores this inalienable element of end to end encrypted platforms. If such platforms are compelled to comply with Section 8, it will become practically impossible for communications service providers to offer end to end encryption, and this will have a debilitating effect on users' human rights and safety.

Any ability created to detect and address encrypted content **will amount to the creation of an exceptional access mechanism, a backdoor, a weakness or a vulnerability in the system**. Once such a mechanism is created, there is no certain way of ensuring that it only works for the authorised parties, be it the government or the service provider. There is simply no such thing as

---

[7] Access Now, *Policy Brief: 10 Facts to Counter Encryption Myths*, https://www.accessnow.org/cms/assets/uploads/2021/08/Encryption-Myths-Facts-Report.pdf
[8]Resolution adopted by the United Nations General Assembly on 16 December 2020 , *The Right to Privacy in the Digital Age*, https://undocs.org/en/A/RES/75/176
[9] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, https://www.undocs.org/A/HRC/29/32
[10] Coalition of NGOs, N*ecessary & Proportionate - on the application of human rights to communications surveillance*, https://necessaryandproportionate.org/principles/

a backdoor that only works for the "good guys". The mechanism will be exploited by malicious state and non state actors and lead to people's privacy and security being severely compromised as well as a weakened cyber security infrastructure vulnerable to attacks.

Further, Section 8 imposes an obligation to identify content that "is or may be unlawful or harmful". There is a critical difference between content detection tools that may identify content that *is* harmful, and those that may additionally also identify content that *may be* harmful. Several communications platforms and cloud storage services, that are not end to end encrypted, use perceptual hashing to identify and prevent the spread of illegal content. Perceptual hashing entails matching media files against a database of known or previously reported illegal images or videos, with a unique hash representing each such image or video. It must be noted that such tools are incompatible with end to end encryption, and raise several concerns for people's rights, freedoms, and safety, owing to their vulnerability against reverse engineering and exploitation, and the possibility of false classifications. Having said that, even such a potentially problematic tool would also only enable the detection of content that *is* illegal. The requirement of detecting content that also *may be* illegal adds an extremely concerning additional layer of obligation. Further, the over broad and ambiguous nature of the term "harmful" will result in amplified and unnecessary policing and censorship of content. Encrypted platforms will be forced to cast a disproportionately wide net, and comb through all the content exchanged by users, leading to an unreasonably expanded scope for surveillance, in clear violation of the principles of necessity and proportionality. As a result, the privacy and security guarantees that are central to the design and purpose of such platforms will be eliminated. Ultimately, people's rights and safety online will suffer.

To be sure, any content detection or moderation tool that enables a third party, including the service provider or law enforcement, to detect, access or address encrypted data without an active and enabling choice by a party to the communication, or otherwise undermines or weakens encryption, is fundamentally in contradiction with end to end encryption. The imposition of a legal obligation on service providers to implement such mechanisms will be antithetical to the Draft BOSE's goals of online safety, privacy and security.

We emphasize that the mandate set out in Section 8 is neither necessary nor proportionate, and will do far more harm than good. It will compel service providers to implement highly intrusive measures that compromise online safety, undermine encryption, expand surveillance, imperil human rights and conflict with democratic principles.

Any proposals for content governance that leads to compromised or weakened end to end

[11] Just Security, *Why An Encryption Backdoor for Just the "Good Guys" Won't Work*, https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

encryption are fundamentally opposed to human rights [2], and the consequences will be particularly grave for at risk users and vulnerable communities including, human rights defenders, journalists, and activists. Further, the importance of secure, end to end encrypted communication cannot be overstated for government, intelligence and law enforcement officials, as well as for enterprises and corporations that rely on such channels to share sensitive information, and indeed for national security and the economy on the whole.

Division 4 on reporting and complaints can be strengthened further:

We support the provisions in Division 4 of the Draft BOSE aimed at enabling and improving clear and identifiable mechanisms for users to report, and make complaints about, unlawful content.

A core principle of content detection tools on end to end encrypted platforms should be that they enhance users' autonomy, place control in the hands of the users and empower them with the ability to report, complain, block and seek support to prevent the recurrence of harmful experiences. Division 4 is aligned with this principle, and Section 8 is not.

Division 4 can be strengthened further. For reporting and complaint mechanisms to enable long term safety, it is important to ensure that service providers have processes in place for creating awareness and equipping users with the knowledge to utilize these tools. Further, several users have reported that they are re contacted by people they have reported or blocked on social media and messaging platforms. [3] Therefore, it is also necessary to implement clear procedures and structures for follow through by the trust and safety teams of such service providers to ensure appropriate categorisation of complaints, report resolution, sustained engagement with users and improved outcomes, in order to prevent such instances. These elements would complement the Draft BOSE's requirements on reporting and complaints and help achieve the goal of online safety.

We emphasize that the application of Division 4 in this manner, in the context of end to end encrypted platforms, is a suitable alternative to Section 8, as it will help address concerns pertaining to unlawful content by empowering users, without jeopardizing their privacy and security.

Summary Recommendations

---

[12] Access Now, *26 Recommendations on Content Governance: A Guide for Lawmakers, Regulators, and Company Policy Makers*, https://www.accessnow.org/cms/assets/uploads/2020/03/Recommendations-On-Content-Governance-digital.pdf

[13] The Verge, *The child safety problem on platforms is worse than we knew*, https://www.theverge.com/2021/5/12/22432863/child-safety-platforms-thorn-report-snap-facebook-youtube-tiktok

Access Now respectfully urges the government to consider the following recommendations:

- Section 8 should be removed from the Draft BOSE, and the government should refrain from incorporating and implementing any provision that would have the effect, directly or indirectly, of breaking, undermining, weakening or circumventing end to end encryption, as this would be detrimental for human rights and in contradiction with the Draft BOSE's goal of online safety.
- At the very least, if Section 8 is not eliminated, the Draft BOSE must clarify that "reasonable steps" in Section 8 would not include any measures that may have the effect, directly or indirectly, of breaking, undermining, weakening or circumventing end to end encryption.
- Further, it must be clarified that services that offer end to end encryption are exempt from the application of Section 8.
- Division 4 of the Draft BOSE should also include guidance on strengthening trust and safety teams to ensure a robust ecosystem of user reporting and complaints that strengthens users' autonomy and ensures effective follow through mechanisms for effective outcomes.

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
[redacted]

Raman Jit Singh Chima
Senior International Counsel and Asia Pacific Policy Director, Access Now
[redacted]

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