ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

700 K Street NW Suite 600
Washington, DC 20001

COMMENTS OF ITIF

to the

Senate Standing Committees on Environment and Communications

Canberra, ACT

In the Matter of: The Online Safety Amendment (Digital Duty of Care) Bill 2026	)	Public Comment

October 30, 2026

CONTENTS

Introduction and Summary 2
Overly Broad Definitions Complicate Compliance 2
Unchecked Enforcement Power Threatens Encryption 3
A Private Right of Action Leads to Frivolous Lawsuits 5
Conclusion 5

INTRODUCTION AND SUMMARY

The Information Technology and Innovation Foundation (ITIF) is pleased to submit these comments to the Senate Environment and Communications Legislation Committee's inquiry into the Online Safety Amendment (Digital Duty of Care) Bill 2026.[1] ITIF is a nonprofit, non-partisan public policy think tank committed to articulating and advancing pro-productivity, pro-innovation, and pro-technology public policy agendas around the world that spur growth, prosperity, and progress.

Governments, parents, and industry all play a role in keeping children safe online. However, measures that require or incentivize companies to protect children from harmful content should balance children's safety with the rights of users of all ages to access lawful content online and engage in private, secure communications. Additionally, obligations on companies should not impose compliance burdens that significantly impede innovation and economic growth or restrict access to online services.

Specifically, Australia should avoid:

- relying on overly broad language that complicates compliance, may encourage censorship, and worsens users' online experience;
- giving the Minister for Communications, eSafety Commissioner, or any other party the power to require or incentivize companies to break or weaken encryption or withhold encryption services from certain users; and
- giving individuals the ability to sue companies directly for online safety violations through a private right of action.

OVERLY BROAD DEFINITIONS COMPLICATE COMPLIANCE

The current version of the Digital Duty of Care Bill attempts to address issues with the exposure draft that could have led to censorship. Specifically, the current version of the bill creates carve-outs to its definitions of "seriously harmful material and conduct" and "material and conduct that is harmful to children" for professional news, public-interest material, research, and public-health information and requires Parliament to

[1] Parliament of Australia, "Online Safety Amendment (Digital Duty of Care) Bill 2026," 15 October 2026, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/DigitalDutyofCare48P.

vote should it wish to expand the bill's definitions. However, the bill's overly broad definitions would impose undue compliance burdens on tech companies seeking to protect children while complying with the law.

Overly broad definitions attempt to shield children from harmful content but often result in the overregulation of digital technologies. To avoid liability, online services may overcorrect and make it more difficult for minors, and potentially all users, to access helpful content related to controversial topics such as mental health, suicide, eating disorders, sexuality, and more. While the bill's definition of "seriously harmful material and conduct" exclusively lists specific types of material and conduct, relying in part on existing legal definitions, its definition of "material and conduct that is harmful to children" is far vaguer and includes the broad subcategory of "any other material or conduct, or combination of material and conduct, that may cause serious harm to children." This leaves companies as the arbiters of what material and conduct is appropriate for children instead of parents, an especially difficult task given that children of different ages have different needs, children mature and develop at different paces, and each child's needs are unique.

The bill's definition of a "digital duty of care" outlines specific steps companies should take to comply with the law, such as preventing access for children below16 to certain design features, conducting risk assessments, providing users with tools to customize certain aspects of their online experience, and implementing age-assurance measures to prevent children's access to adult content. It requires companies to take "appropriate action" to ensure a safe online environment and "effective measures" to mitigate risks identified in risk assessments and provides guidance on how to determine what is appropriate and effective. This is less vague and nebulous than, for example, the duty of care for online services in some versions of the United States' proposed Kids Online Safety Act.[2] However, the concept of a digital duty of care remains vague and undefined by existing case law and thus remains a significant compliance burden.

Finally, the bill singles out design features that have "negative behavioural impacts." It singles out recommendation algorithms ("recommender features"), infinite scrolling ("endless-feed features"), engagement metrics ("feedback features"), and ephemeral content ("time-limited features"). There is very limited scientific research into the harmful potential of specific design features. In the absence of concrete evidence, policymakers lean more heavily on the perception of addictiveness, which leads to regulations such as the proposed Digital Duty of Care Amendment that arbitrarily single out design features that contribute to a more engaging or convenient online experience—the primary purpose of many online services. Punishing online services for providing their users with engaging, convenient experiences hinders innovation and ultimately punishes users.

UNCHECKED ENFORCEMENT POWER THREATENS ENCRYPTION

Regulations such as the Online Safety Act and the proposed Digital Duty of Care Amendment can pose a risk to encryption services. Australia should avoid giving the Minister for Communications, eSafety Commissioner, or any other party the power to require or incentivize companies to break or weaken encryption or withhold encryption services from certain users, including teenagers.

[2] "S.1748 - Kids Online Safety Act," Congress.gov, accessed 28 October 2026, https://www.congress.gov/bill/119th-congress/senate-bill/1748/text.

Encryption, particularly end-to-end encryption (E2EE)—a form of encryption in which only the parties sending and receiving an encrypted message can decrypt it—has repeatedly found itself at the centre of the online safety debate. Privacy and security experts, civil liberties advocates, and tech companies argue for the importance of encryption to protect private communications and sensitive data, while law enforcement agencies claim that encryption makes their jobs more difficult. However, regulatory efforts to weaken encryption ultimately harm law-abiding individuals of all ages far more than criminals.

Various law enforcement agencies have advocated for mechanisms that would allow governments to access encrypted communications under lawful authority. These mechanisms can introduce security risks that bad actors can use to circumvent encryption. No technical mechanism can guarantee that access to encrypted communications granted to authorities will be used only for lawful purposes while eliminating the risk of unauthorized access. Any mechanism that enables exceptional access can create additional vulnerabilities that malicious actors may exploit: Any door that opens for the "good guys" can also open for the "bad guys."

There are far more law-abiding individuals who reap the privacy and security benefits of encryption than there are criminals who use encryption to evade law enforcement. Vulnerable individuals, including victims of abuse and the LGBTQ community, use encryption to communicate privately and seek support without fear of reprisal.[3] Journalists also use encrypted messaging services to communicate with confidential sources.[4]

Encryption is also an important tool for children, protecting their privacy and security and giving them the agency to explore sensitive topics without fear of surveillance. [5] Restricting children's access to encrypted services assumes that every child lives in a safe, supportive home environment, but unfortunately, many do not. The Australian Child Maltreatment Study, published in 2023, found that 62.2 percent of the Australian population has experienced at least one type of child maltreatment, including physical abuse, sexual abuse, emotional abuse, neglect, and exposure to domestic violence.[6]

Meanwhile, efforts to weaken commercial encryption will not eliminate law enforcement's concerns surrounding crimes against children. Individuals who have already demonstrated a willingness to break the law will not restrict themselves to providers that comply with the law. Some criminals may continue to use less secure technologies, especially in the short term before alternatives become more widely adopted, which would make it easier for law enforcement to gain access to some information.

---

[3] "Fact Sheet: Understanding Encryption: The Connections to Survivor Safety," Internet Society, 18 December 2020, https://www.internetsociety.org/resources/doc/2020/understanding-encryption-the-connections-to-survivor-safety/; "Encryption: Essential for the LGBTQ+ Community," Internet Society, 1 November 2019, https://www.internetsociety.org/resources/doc/2019/encryption-factsheet-essential-for-lgbtq-community/.

[4] "Fact Sheet: How Encryption Can Protect Journalists and the Free Press," Internet Society, updated 7 September 2022, https://www.internetsociety.org/resources/doc/2020/fact-sheet-how-encryption-can-protect-journalists-and-the-free-press/.

[5] Sharayah Lane, "Encryption is a Preventative Tool that Protects Children," Internet Society, 19 July 2024, https://www.internetsociety.org/blog/2024/07/encryption-is-a-preventative-tool-that-protects-children/.

[6] Ben Matthews et al., "The Australian Child Maltreatment Study: National prevalence and associated health outcomes of child abuse and neglect," *The Medical Journal of Australia* 218, no. 6 (April 2023), S19, https://www.mja.com.au/journal/2023/218/6/supplement.

However, if domestic providers cannot offer true E2EE, criminals can find tools from open-source software or foreign providers. If they have the technical proficiency to do so, they can even build their own, since encryption methods are now in the public domain. When bad actors use foreign tools, domestic law enforcement agencies lose access to metadata from domestic providers, making it more difficult for these authorities to monitor crime.

Law enforcement has alternative investigative methods that can obtain information related to encrypted communications without breaking the encryption itself. These include collecting non-content metadata, seizing and accessing devices to retrieve locally stored messages, obtaining unencrypted cloud backups, relying on human informants, and using investigative tools to capture keystrokes or screenshots before messages are encrypted or after they are decrypted on a device.

A PRIVATE RIGHT OF ACTION LEADS TO FRIVOLOUS LAWSUITS

Australia should avoid giving individuals the ability to sue companies directly for online safety violations through a private right of action. This would open the floodgates for unnecessary, baseless lawsuits against organizations that fall under the Online Safety Act's purview, which would disincentivize organizations from offering innovative new products or services that may open them up to liability.

Proponents of a private right of action frame it as a gift to consumers, providing them with access to remedies against organizations that have violated their rights. However, even in the case of legitimate lawsuits, the payouts are often small, and attorney fees are often high. Ultimately, lawyers are the only group that would significantly benefit from a broad private right of action. Meanwhile, the Australian economy would suffer as the high cost of litigation dramatically drives up costs for companies, diverting funds away from innovating and creating new products and services.

Consumers would also suffer as companies pass these costs along to them by driving up prices, charging for services that were previously free, or offering discounts less frequently.[7] Evidence shows that companies pass on compliance costs to consumers in order to reduce the impact they would have on their business. This can come in the form of either raising prices for paid services or charging for services that were previously free. Researchers from the United States and United Kingdom found in 2019 that, across all industries, federal government regulations lead to higher consumer prices, and that this disproportionately impacts low-income households.[8]

CONCLUSION

Protecting children online and preserving the benefits of a free, secure, and innovative digital world should not be competing goals. To that end, Australia should adopt policies that are narrowly targeted to demonstrable harms, provide companies with clear and workable compliance obligations, and preserve strong

[7] Ash Johnson and Daniel Castro, "Maintaining a Light-Touch Approach to Data Protection in the United States" (ITIF, August 2022), https://itif.org/publications/2022/08/08/maintaining-a-light-touch-approach-to-data-protection-in-the-united-states/.

[8] Dustin Chambers, Courtney A. Collins, and Alan Krause, "How do federal regulations affect consumer prices? An analysis of the regressive effects of regulation," *Public Choice* 180 (2019): 57–90, https://doi.org/10.1007/s11127-017-0479-z.

encryption for users of all ages. Otherwise, lawmakers will risk creating unintended consequences that harm the very users these policies seek to protect, while imposing costs on consumers, companies, and the economy and stifling innovation.

Thank you for your consideration.

Ash Johnson
Senior Policy Manager, ITIF

Alex Ambrose
Senior Policy Analyst, ITIF