

Consumer Choice Center Comments on the Online Safety Amendment (Digital Duty of Care) Bill 2026

29 October 2026

**Committee Secretary
Senate Standing Committees on Environment and Communications
PO Box 6100
Parliament House
Canberra ACT 2600**

The **Consumer Choice Center** is an independent, non-partisan consumer advocacy group championing the benefits of freedom of choice, innovation, and abundance in everyday life. We champion smart policies that promote growth, lifestyle choice, and defend technological innovation.

Herein, we offer our comments on the Online Safety Amendment (Digital Duty of Care) Bill 2026, as passed by the House of Representatives on 28 October 2026, from a consumer-focused perspective.

General Views on the Bill

The Bill does two very different things. Schedule 1 makes targeted changes to the existing complaints-based schemes: it lets the eSafety Commissioner order the removal of apps built to generate fake nude images, require search engines to delist intimate images and abusive material, and shorten takedown deadlines. Schedules 2 and 3 are far more ambitious. They repeal the Basic Online Safety Expectations and the online content industry codes and standards, and replace them with a single, overarching “digital duty of care” that applies to almost every online service used by Australians, backed by civil penalties of up to approximately \$109 million per contravention.

The Consumer Choice Center shares the goal of protecting Australians, and especially children, from genuinely illegal and abusive material online. Non-consensual intimate images, child sexual abuse material and apps designed to “nudify” real people cause serious harm. Targeted powers to deal with them, subject to proper safeguards, are a reasonable use of government authority.

However, we are sceptical that a broad, open-ended duty of care is the right tool. Duty-of-care models sound appealing in a press release, but in practice

they hand regulators near-unlimited discretion over how lawful products are designed, push companies to remove lawful speech to avoid liability, and put the privacy and security of every user at risk, adults included. In the United States, we have [opposed](#) the “duty of care” in the Kids Online Safety Act for the same reasons: it shifts decisions about what young people see and do online away from parents and towards government officials, and degrades the experience for all users. Australia’s version is broader than anything proposed in Washington.

We focus on five areas: the vagueness and scope of the duty itself; its treatment of design features and parental choice; its implications for encryption and private communications; the age assurance mandate; and the expanded powers of the eSafety Commissioner.

A Duty Without Limits

Section 26 requires every person responsible for an online service to “take appropriate action to ensure a safe online environment”. Section 25C defines that as an environment in which Australians “are protected” from seriously harmful material and conduct, and children are protected from material that is “harmful to children”. This is an obligation to guarantee an outcome, not to follow a defined process. No service that hosts user content, from a global platform to a local community forum, can guarantee that outcome. Every service will therefore be in technical breach at all times, and the only real question will be whether the Commissioner chooses to act.

The categories of material that services must shield children from are also open-ended. Alongside clearly defined harms, section 25E includes material that “glorifies crime”, material that “encourages or promotes hostile attitudes towards women or gender equality”, and a catch-all of any other material or conduct “that may cause serious harm to children”. Reasonable people disagree about where these lines fall. Because platforms cannot reliably tell which users are children, adults’ lawful speech will be restricted too. And because the Bill heavily penalises under-removal while imposing no consequence for over-removal, the rational response for any risk-averse company is to take down more content, not less.

Much of what the duty will actually require has not yet been written. The Minister may decide by legislative instrument which services count as “social media services”, which design features have “negative behavioural impacts”,

and which services are exempt. The Commissioner may set the content, standards and frequency of risk assessments and publish guidelines on compliance. Parliament is being asked to approve a framework whose real substance will be filled in later by the executive and by the regulator itself.

The scope of the duty is extraordinary. Under section 25B it applies not only to social media, but to messaging and email services, search engines, app stores, hosting and cloud storage providers, generative AI services, internet service providers, and anyone who “manufactures, supplies, maintains or installs” equipment that connects to the internet. That captures phone makers, router manufacturers and the technician who installs a home modem.

Most strikingly, section 26A(3) provides that, in deciding whether measures are appropriate or effective, “the cost of the action or measures must not be taken into account”. Every regulation has costs, and consumers ultimately pay them through higher prices, fewer features and fewer choices. Large incumbents can absorb the compliance teams, annual risk assessments retained for six years, transparency reports and audits the Bill demands. Australian start-ups, small forums, open-source projects and new entrants cannot. A law that forbids the regulator from considering cost will entrench the very largest platforms and reduce competition and choice for Australian consumers.

Penalties compound the problem. Breaching the duty, or the age assurance or risk assessment obligations, attracts a maximum of 60,000 penalty units, which one [legal analysis](#) puts at approximately \$109 million per contravention for a corporation, and continuing contraventions can be counted day by day. Paired with a vague standard, penalties of this size will chill innovation and may lead some services to withdraw features, or withdraw from Australia altogether.

Design Features and Parental Choice

Section 25G declares by statute that “recommendation features,” meaning any feature that selects content based on information associated with a user’s account, and “logged-in features” such as endless feeds, like counts and disappearing content, have “negative behavioural impacts”. On social media services, children under 16 must not have access to or be exposed to these features at all, and the Minister may add further features to the list.

Personalised recommendations are what make modern apps useful: they help users find music, educational videos, news and communities that match their interests. Whether a 15-year-old should see a personalised feed is a decision for that teenager's parents, not the Minister. Australia already imposes a social media minimum age of 16 for accounts on age-restricted platforms; this Bill goes further and regulates the design of every service a young person can use. Parents already have powerful device-level and app-level controls. Government should support digital literacy and those tools, rather than substituting its own judgement for that of Australian families.

We do note one positive element. Section 27A's user empowerment tools, which give users control over how features such as recommendations operate, are in principle consistent with consumer choice. Choice is best served, however, when such tools are offered competitively in response to consumer demand, not mandated feature by feature through ministerial instruments.

Encryption and Private Communications

Our most serious concern is the Bill's impact on encryption. The word "encryption" does not appear anywhere in the Bill, yet the duty applies to "relevant electronic services" such as messaging apps and email, to hosting and cloud storage, and to device manufacturers. In judging whether a service has done enough, section 26A(1)(b) asks how far its measures reduce the risk that the service will be used to "solicit, generate, access, distribute or store" seriously harmful material.

An end-to-end encrypted service cannot see what its users send or store. The only way for it to "reduce the risk" that particular material is distributed or stored is to inspect content on the user's own device before it is encrypted, known as client-side scanning, or to weaken the encryption itself. Both are backdoors. As we set out in our recent submission to the Parliamentary Joint Committee on Intelligence and Security, there is no way to turn off encryption for some without turning it off for all. As Apple told this Parliament in its 2018 [submission](#), "Encryption is simply math."

The Bill offers three apparent safeguards. None is adequate.

First, section 26A(1)(d) lists "the impact on the security of the online service" as one matter to be taken into account. Security is merely a factor to be weighed against a "safe online environment", not a limit. By contrast, section

317ZG of the *Telecommunications Act 1997*, inserted by the Assistance and Access Act in 2018, expressly prohibits requiring a provider to build a “systemic weakness” or “systemic vulnerability” into its systems. Even that contentious law contained a clear encryption safeguard; this Bill contains none. Worse, Schedule 3 repeals the existing online content industry codes and standards, including the protections they gave end-to-end encrypted services, without replacing them.

Second, section 26B states that the duty does not require action “in relation to lawful communications occurring in private solely between consenting adults”. This is far narrower than it looks. A provider cannot know whether a communication is “lawful” without examining its content, and cannot know a conversation is “solely between consenting adults” without verifying the age of every participant. The exception does not cover a family group chat that includes a teenager, or files kept in an encrypted cloud backup. All of these fall back within the full duty.

Third, the Commissioner’s remedial directions under section 26E can be reviewed by the Administrative Review Tribunal, but only after the fact. A direction may require any “specified action” towards compliance, non-compliance carries its own penalty, and nothing in the Bill prevents a direction from requiring the scanning of private messages. Separately, section 28A allows the Commissioner to require a provider to give a nominated person “access to the service” to report on its systems, which is itself a security risk.

These are not abstract concerns. In 2024, Chinese state-backed hackers known as Salt Typhoon breached major United States telecommunications networks, reportedly including systems built for lawful interception. In response, the US Cybersecurity and Infrastructure Security Agency [advised](#) highly targeted individuals to use only end-to-end encrypted communications. Access built for the “good guys” becomes a target for everyone else. In 2021, Apple announced, and later abandoned, a plan to scan photos on users’ devices after security researchers warned it could be repurposed. And in February 2025, Apple [withdrew](#) its Advanced Data Protection feature for new users in the United Kingdom following a government order, leaving British consumers with weaker security than consumers elsewhere.

Encryption protects Australians' banking, health records, business secrets and family conversations, as well as political dissidents who have sought refuge here from hostile foreign governments. Signal has already said it would leave Australia rather than undermine its encryption. If Australians lose access to secure services, they will not be safer. They will be easier targets for criminals and foreign intelligence services.

Age Assurance and the Creation of Data Honey pots

Section 27D requires any online service where there is a “reasonably foreseeable risk” that a child could access pornography to offer at least two age assurance methods and implement access controls. Given the breadth of “online service”, that threshold could be met by search engines, messaging apps, cloud storage, AI chatbots and many general-purpose websites. In practice, Australian adults will be asked to prove their age far more often, to far more companies.

Every age check creates data, and every database of identity documents is a target. In October 2025, Discord disclosed that around [70,000 users' government ID photos](#) were exposed when a third-party vendor handling age verification appeals was breached. Australians need no reminder of the consequences: the 2022 [Optus](#) breach exposed the personal information of 9.5 million people, including passport and driver's licence numbers, and the [Medibank](#) attack the same year saw sensitive health data published on the dark web. A law requiring age assurance across the internet will multiply these risks.

An Expanding Regulator

The Bill substantially expands the eSafety Commissioner's powers with limited checks. New section 177A gives the Commissioner power to do “all things necessary or convenient” for the Commissioner's functions. Schedule 2 adds the Commissioner to the Privacy Act's definition of an “enforcement body”, making it easier for organisations to disclose Australians' personal information to the Commissioner, and Schedule 1 allows the Commissioner to share information with any Commonwealth entity. New compulsory examination powers carry up to 12 months' imprisonment for non-compliance. The Commissioner and approved researchers may also operate fake “sock puppet” accounts on any service, despite its terms of use, with immunity from civil proceedings.

Schedule 1, Part 5 retrospectively validates industry codes and standards that were registered without the required public consultation, deeming them “never to have been affected” by that failure. Consultation requirements protect the public’s right to be heard. Retrospectively excusing a failure to follow them sets a poor precedent, and sits uneasily alongside a Bill that asks Parliament to trust the same regulator with far greater discretion. Likewise, the new definition of “reposted” material in Schedule 1, which captures material where “text, dialogue or commentary” has been changed, risks sweeping in legitimate commentary and reporting under 24-hour takedown deadlines.

Our Recommendations

1. Insert an express encryption safeguard, modelled on section 317ZG of the *Telecommunications Act 1997*, providing that nothing in the digital duty of care, a risk assessment requirement, a remedial direction, guidelines or any instrument may require a provider to build a systemic weakness or vulnerability, create a decryption capability, or scan the content of end-to-end encrypted communications or storage, including on a user’s device.
2. Broaden the exception in section 26B to cover all private and encrypted communications and private storage, regardless of participants’ ages, and remove any requirement for providers to judge whether communications are “lawful”.
3. Replace the outcome-based duty to “ensure” a safe online environment with an obligation to take reasonable and proportionate steps against clearly defined illegal material, and remove the open-ended categories in section 25E.
4. Delete section 26A(3) and require that the costs of measures, including costs to consumers and effects on competition, be taken into account.
5. Remove internet carriage services and equipment manufacturers, suppliers and installers from the definition of “online service”.
6. Remove the statutory designation of recommender and logged-in features as having “negative behavioural impacts”, and support parental controls and digital literacy instead of mandated design restrictions.

7. Require age assurance to be privacy-preserving, prohibit the retention of identity documents, and guarantee that no Australian must provide government identification to access lawful services.
8. Remove the eSafety Commissioner from the Privacy Act definition of “enforcement body”, and remove the retrospective validation in Schedule 1, Part 5.
9. Require an independent review of the digital duty of care within two years of commencement, covering its effects on privacy, security, speech and competition.

Conclusion

Australians rightly expect the online services they use to take illegal and abusive content seriously, and the Consumer Choice Center supports targeted, evidence-based measures to deal with it. But the digital duty of care is not targeted. It imposes an unachievable obligation on almost every online service in the country, forbids the regulator from weighing its costs, leaves the detail to be decided later by the Minister and the Commissioner, and offers no meaningful protection for encryption.

The likely result is not a safer internet, but a more expensive, more censored and less secure one, with fewer services available to Australian consumers and more of their personal information sitting in databases waiting to be breached. We urge the Committee to recommend the amendments above and, above all, to ensure that no Australian loses access to secure, encrypted communications in the name of online safety.

Yours faithfully,

Yaël Ossowski
Deputy Director
Consumer Choice Center