From the desk of Dr Andrew Bushnell, Senior Fellow
abushnell@ipa.org.au

Institute of Public Affairs

30 October 2026

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

Dear Committee Secretary

The digital duty of care bill would create a censorship machine built on arbitrary government decision-making, opaque controls, and surveillance of users.

The purpose of this submission is to provide an analysis of the *Online Safety Amendment (Digital Duty of Care) Bill 2026* (the bill), which would enact the Albanese government's *digital duty of care*, a regulation of online services through an enforceable obligation to provide users with a "safe online environment" that protects them from certain kinds of "material and conduct", risks that are "reasonably foreseeable", and the effects of various "design features" like algorithmic feeds.[1]

Building upon a substantial body of research by the Institute of Public Affairs (IPA), summarised at Appendix A, this submission finds:

1. The regulatory architecture of the bill would give government extraordinary direct and indirect control over content on the internet.
2. The wide scope of the duty entails extraordinary and opaque discretionary powers for government.
3. Despite changes to the bill, the harm provisions still endanger freedom of speech, including by incentivising further age-gating of the internet.
4. The bill's risk provisions will powerfully influence the governance of online services and the rules under which Australians communicate and organise politically online.
5. Government-mandated user empowerment tools are not neutral in their effects on content and will likely affect the circulation of news and information online.
6. The operation of the digital duty of care will reinforce its censorious design by incentivising over-compliance through heavy penalties and cultivating services' dependence on government guidance to understand their obligations.
7. The digital duty of care would establish a surveillance regime in service of propagating ever more sophisticated controls over content and features.
8. The government's open political ambitions for the proposed law mean it cannot be trusted with the powers contained in the bill.

The danger of this bill for freedom of speech therefore emerges directly from the regulatory architecture and operational incentives that the bill would create, so it cannot be removed from, or managed within, that proposed framework. Accordingly, this submission recommends that the bill be withdrawn and this regulatory approach be abandoned.

IPA Board of Directors: Geoff Hone AM – Chairman, Scott Hargreaves – Executive Director
Dr Michael Folie AM, Dr Tim Duncan, Michael Hickinbotham, Rebecca Clough, Lesley Gillespie OAM, Simon Fenwick, James Power
IPA Honorary Life Members: Mrs Gina Rinehart AO, The Hon. Rod Kemp AM, Dr Bryant Macfie, Mr Charles Goode AC, Mr John Roskam

1. The regulatory architecture of the bill would give government extraordinary direct and indirect control over content on the internet.

The digital duty of care is built around three interlocking mechanisms for controlling and influencing content online:

- *The harm provisions*: The object of the duty (at s 26) is that online services ensure a "safe online environment", which, per s 25C, is one in which people are protected from material and conduct that is seriously harmful (s 25D), and children under 18 years of age are protected from material and conduct that is harmful to children (s 25E), "harms associated with … design features", and, on social media services, children under 16 years of age are protected from features' "negative behavioural impacts" (s 25G).
- *The risk provisions*: The obligations of the duty are that online services take "appropriate action" to ensure a safe online environment, including taking "effective measures to mitigate risks identified in risk assessments". Per s 26A, appropriate and effective are determined by reference to the extent to which actions would achieve a safe online environment and reduce the risk of people being exposed to the various statutorily defined harmful materials.
- *The user empowerment tools provisions*: Online services are also obliged, per s 27A, to comply with any legislative instruments ordering the adoption of certain "user empowerment tools" that the Minister deems "necessary to protect users … from harms associated with access or exposure to a design feature of the service".

Together, these different mechanisms create a censorship machine. The threat of censorship emerges from the wide scope of the duty and inheres in all the different parts of the scheme and how they interact. That is, the threat goes beyond the direct controls the bill would give government over harmful content and includes the powers of government to influence how content circulates online. This includes the risk and user empowerment tools provisions, which, while facially neutral as to content, will necessarily influence what Australians can access and share online.[2] It also includes the way compliance with the duty will be enabled and enforced.

2. The wide scope of the duty entails extraordinary and opaque discretionary powers for government.

The government has adopted the approach – recommended in the 2024 independent review of the *Online Safety Act 2021* – of applying a single overarching duty across the internet. The reviewer recommended this on the grounds that it would place the onus on online service providers to move from "reactively tackling specific pieces of material" to "taking a preventative and system-based approach".[3] Consistent with this, and with the exposure draft, the digital duty of care will apply, per s 25B(1) of the bill, to almost the entire internet: internet service providers, hosting services, search engines, websites, social media platforms, AI tools, and email and messaging services.

The wide scope of the digital duty of care means that how it operates in practice will largely be determined by discretionary decisions of the Minister (including that s 25B(3) gives the Minister the power to exempt services from the duty) and eSafety Commissioner, as well as the decisions of the regulated services themselves. For example, the bill's explanatory memorandum notes that "Not all service providers have the same risks of harm … but all

services hold the obligation to provide a safe online environment under their Duty", while also suggesting a responsive approach to enforcement, "It is intended that the Commissioner will exercise regulatory discretion in determining the appropriate enforcement option …".[4] And as discussed further below, the bill also gives the Minister and Commissioner various discretionary powers to do with the regulation of design features, risk assessments, and data access.[5] Online services, too, will also have to make decisions about how they manage their assessed risks, including how their platforms interact with other services.

For Australian internet users, the wide scope and associated discretionary powers mean that the full effects of the digital duty of care are impossible to anticipate, will be difficult to track as they develop, and will be the products of decisions over which they have no influence.

3. Despite changes to the bill, the harm provisions still endanger freedom of speech, including by incentivising further age-gating of the internet.

Regarding the harm provisions, it should be noted that based on feedback to the exposure draft, including from the IPA, the government has dropped provisions relating to the safe online environment standard that would have given the Minister powers to add new categories of harmful material and conduct. The government has also added wide-ranging exclusions to the categories of seriously harmful material and conduct, comprising "professional news material" and material in the "public interest" as well as all "Class 2 material" (defined in s 107 of the Act), meaning that these kinds of materials cannot be harmful under the statutory standard.

While these changes are improvements, the harm provisions still pose a danger to freedom of speech. The government will have considerable discretion to determine whether actions taken to address the statutorily defined harmful material and conduct are appropriate (s 26A) and through the power to issue remedial directions about "specified action[s]" to create a safe online environment (s 26E). This will include making determinations about the extent to which services' actions achieve or would achieve a safe online environment, the nature of the material in question and the extent to which it is unsafe, and how reasonable and proportionate the actions are to harms and the risk of harm.

For users, then, the full effect of the harm provisions will be determined by administrative decisions that are opaque and made by largely unaccountable bureaucrats and online services compliance teams.

The bill also retains the distinction between adult and child users. As the IPA pointed out in our submission on the exposure draft, one effect of this will be that many online services may have to choose between age-gating and childproofing. For example, search engines and AI tools may implement age verification checks that must be passed by users seeking access to full results or features. But for many online services, it may be more efficient to adhere to the childproof standard instead. This may be attractive for smaller services, like personal websites, and services that have little direct contact with users, like hosting services. Extending age verification across large parts of the internet will therefore place a barrier between adult users and content and functionality they may want to access, and some users may be deterred from engaging in online activity they otherwise wanted to undertake.[6]

This has already been seen in the case of gaming platform Steam, which has introduced age verification based on credit cards. Many Australians, especially young gamers, do not have credit cards, and so are excluded from the full functionality of that platform.[7]

It is also notable that the harm provisions related to children are often broad and politically contentious. For example, s 25E(1)(c) defines as harmful to children material or conduct encouraging or promoting hostile attitudes towards gender equality, which, on its face, might seem to capture traditional religious teachings (about, say, the complementarity of the sexes). Additionally, s 25E(1)(f) provides a catch-all for "any other material or conduct … that may cause serious harm to children", and while this provision uses the higher "serious harm" standard, the explanatory memorandum holds that s 25E is overall "not … intended to create an exhaustive list of harms".[8] The importance of this lies in the potential for eSafety to expand the reach of s 25E administratively, without proper scrutiny, which would apply to adult users in childproofed online environments.

4. The risk provisions will powerfully influence the governance of online services and the rules under which Australians communicate and organise politically online.

The risk provisions provide a powerful mechanism for government decisions to influence the content and distribution of content online.

Indeed, these provisions are the real heart of the digital duty of care, because they provide the mechanism by which the duty anticipates emerging risks of harm and is how the government intends to implement what the statutory review calls "an ongoing cycle of risk identification and assessment" and the explanatory memorandum calls "proactive and ongoing action".[9]

The most important point to note about the bill's risk assessment process is that it is broader than the statutorily defined harms. Section 27 requires all online services to undertake written risk assessments that identify "reasonably foreseeable" risks of harm associated with material, conduct design features, systems, and processes, and potential impacts on persons. This contemplates risks beyond those of the statutory harms. As such, the exclusions from the definitions of harmful content will not limit what kinds of content is relevant to the risk assessment process.

For example, the explanatory memorandum discusses "cumulative harms". It states,

> This includes, for example, a sustained campaign which may involve hundreds of individually brief, implicit or indirect abusive communications being sent or directed to the same person or organisation by multiple users, which may, when considered in isolation, not meet the threshold of harm.[10]

It can be accepted that coordinated abuse may warrant intervention by services, but it is not always easy to distinguish between such abuse and mere widespread criticism. Australians are entitled to be wary here given, for example, that the Commonwealth Secretaries Board recently requested a ban on sharing clips of them from parliamentary hearings on social media, which exposes them to ridicule.[11] Because the risk provisions are not limited to the statutory harms, it is possible that measures such as those requested by these senior bureaucrats could be urged upon services by government guidance and rules.

It is notable, then, that the risk provisions, including the definition of appropriate and effective at s 26A, are effectively unlimited regarding what they can consider and affect.

These provisions:

- Do not separately provide protections for freedom of speech or even news coverage.
- Drop the exposure draft's listing of user privacy as a relevant consideration for risk management.
- Expressly exclude, at s 26A(3), "the cost of the action or measures must not be taken into account" as a relevant consideration in determining appropriate and effective actions and measures.

In practice, the management of identified risks will significantly influence how services operate and, consequently, what content users can access on them. The explanatory memorandum notes "terms of service, community standards and guidelines, complaints handling mechanisms" and "detection and intervention capabilities" and "content moderation" as possible means for services to manage risks.[12]

The overall intention seems to be that the risk assessment process should be as expansive as possible, capturing as many risks and leading to as many effective measures as online services, in conjunction with eSafety, can identify.

Put simply, then, the risk assessment process will powerfully influence the rules under which Australians communicate online.

5. Government-mandated user empowerment tools are not neutral in their effects on content and will likely affect the circulation of news and information online.

Similar indirect effects on content online are possible under the user empowerment tools provisions.

The duty itself regulates design features' effects on under-18s. But in addition to the duty, s 27A(1) gives the Minister the power to order services to adopt user empowerment tools for all users, including adults. In exercising this power, per s 27A(4), the Minister would be prohibited from considering "any material that has been, is or will be accessible to, or delivered to, a user using the service".

However, this safeguard does not mean that these orders must be neutral in their effects on content. The definition of "user empowerment tool" at s 27A(5) expressly provides that such a tool enables users to manage design features "including, for example, by providing control over the kind of content that is recommended to the user", and s 27A(2) provides that Ministerial orders regarding user empowerment tools may be made "by reference to any matter".

At the very least, then, the bill contemplates government intervention into the default settings of online services, with users having to opt-in to see a wider range of content.

But orders under s 27A(1) might also direct how recommender features and other types of design features distribute content; for example, an order might require that content about current news events be dispersed within a content feed, if the Minister is satisfied that such an

order would protect users from "doom-scrolling" (continuous viewing of bad news) or "rabbit holes" (obsessively going deeper into a subject).

In fact, the connection between ostensibly neutral rules governing design features and content has been made by the government in its public messaging about its *My Feed, My Way* initiative. This will be the first legislative instrument made under s 27A(1) should the bill pass and would require social media services to give users the option to toggle between a recommended feed and a following feed comprising only accounts users have chosen to follow, apart from advertising.[13] In its public communications, the government has repeatedly linked this initiative to certain kinds of content that it considers problematic and to its political concerns. On 27 October, the Prime Minister told Parliament that the initiative is part of his government's response to the role of social media in "Turbocharging anger to the detriment of our social cohesion and our democracy", while also "promoting misogyny".[14] Minister Wells has said that "Platforms are not passive – they decide what is amplified, what captures us, which behaviours get rewarded", which essentially concedes that whatever rules govern platforms, they are not neutral, government rules included.[15]

This danger is heightened by the interaction of the duty's mechanisms. For example, the combined effect of age verification, expansive risk management, and government-ordered design features on some online services would radically change the experience of users, who may find news and other information dispersed within "safety-first" feeds that they have to verify their age, and perhaps identity, to access. In this way, the bill would give the government the opportunity to regulate supposed misinformation and disinformation indirectly, by influencing how services operate to distribute information online.

Moreover, as the IPA has said since the digital duty of care was first announced, while orders like *My Feed, My Way* are framed as giving users greater choice, it remains the case that whatever settings users select, their online environment must be "safe", as defined by government. Users cannot opt out of the digital duty of care itself.

6. The operation of the digital duty of care will reinforce its censorious design by incentivising over-compliance through heavy penalties and cultivating services' dependence on government guidance to understand their obligations.

The digital duty of care censorship machine proposed in the bill would be backed by a compliance regime that is designed to incentivise online services to over-comply with their duty, erring on the side of excluding and restricting content.

This incentive comes, in part, from the bill's severe penalties. Breaches of the duty (per s 26C), and failure to conduct risk assessments or comply with orders regarding user empowerment tools (per s 27B), carry penalties of up to $109 million for bodies corporate. The explanatory memorandum explains that these penalties can accumulate if services remain in breach.[16] It is also the case that the penalties may be levied separately (though not for the same conduct).

But the incentive to over-compliance does not lie only in the severity of these penalties. The government will also have tremendous power to shape compliance through guidance and rules, which, because of the wide scope of the duty and the complexity of the regulatory domain, online services will be strongly incentivised to adopt.

The digital duty of care is designed to be proactive, meaning that online services are obliged, to the extent possible, to avoid harms and risks before they even arise. Online services will therefore have to make compliance decisions under considerable uncertainty. They will have to anticipate harms and risks, judge their likelihood and magnitude, and assess the appropriateness and effectiveness of any steps they may take. In this, they will be heavily dependent on guidance and rules issued by government, as well as informal engagements with eSafety to test their compliance steps, regarding their governance (like terms of service), features, and steps taken to ensure a safe online environment.

This operational uncertainty and dependence on government advice is heightened by the interactions of online services with one another. Hosting services host websites which post content built by apps, including AI tools, which then gets shared on social media, which links to sites … and so on. In assessing their own risks, online services will need to consider their interactions with other services and their risks.

As such, online services will not only require guidance about their own compliance but also will have an interest in eSafety providing guidance across the internet, which will give services some assurance about how other services are governing their obligations and risks.

Presumably for reasons like these, this kind of convergence by services on common standards is anticipated by the bill: s 27(4) gives the Commissioner the power to prescribe best practice benchmarks for services, s 28 permits the Commissioner to publish guidelines for complying with the duty, s 166B makes it a function of the Commissioner to develop guidelines regarding best practice, and s 192B(2)(b) identifies "industry best practice" as a relevant consideration for transparency reporting.

Online services will also have limited means to push back upon government recommendations. Section 26A(3) explicitly excludes the cost of compliance from considerations regarding what is appropriate and effective. Similarly, again, there are no protections for freedom of expression or user privacy that government or services must consider in determining what actions and measures services must take to comply with the duty and other statutory obligations.

In sum, then, because the digital duty of care is an overarching obligation across the internet, it will encourage services across the internet to adopt the same, government-recommended, standards.

Moreover, all these engagements between eSafety and these decisions by online services will be opaque to Australian internet users. So not only will government have considerable influence over the operations of online services, but this influence will also be largely hidden from democratic scrutiny.

7. **The digital duty of care would establish a surveillance regime in service of propagating ever more sophisticated controls over content and features.**

Beyond direct compliance measures like these, the bill also sets up a surveillance regime for services and users, aimed at detecting emerging risks and testing how services respond to changing patterns of user behaviour.

One concerning aspect of this regime is that eSafety and "approved researchers" will be permitted, per Division 3 of the bill, to set up fake accounts, called "sock puppets" and operate them on online services "for the purposes of performing the Commissioner's functions" and "undertaking online safety related research". These provisions remain broad and open to abuse, despite the addition of safeguards absent from the earlier exposure draft, including requirements for the eSafety Commissioner to consult with the AFP Commissioner in making policy governing sock puppet use and to publish an annual report on how sock puppets have been used.

For example, ss 205K(e) and (f) permit sock puppet use for "testing" features of services and services' responses to user actions. The explanatory memorandum does not explain what testing might comprise. It would seem, however, to include distributing material and undertaking conduct to observe whether and how services distribute or restrict it, including, it stands to reason, material and conduct that is prohibited by law or services' terms of service.

The sock puppet provisions are just one part of a larger regulatory architecture designed to give eSafety more information about, and therefore more influence over, services compliance actions and measures.

Under the data access scheme established at s 205C, approved researchers may be given access to data regarding "the decision-making algorithms of a feature, system or process". This complements s 28A, which provides that the Commissioner may require services to disclose "information in relation to the functions of a feature, system or process". The explanatory memorandum notes that this latter power is "not intended" to require disclose by a service of its "algorithm", but even if that is true (and it is not clear from the wording of the bill), this proprietary information can still be required to be shared with approved researchers.

More alarmingly still, the bill also provides for the amendment of the *Privacy Act 1988* to include the eSafety Commissioner as an "enforcement body" for the purposes of that Act. This would mean that services are exempted from various privacy considerations in sharing user information – including their personal details, like political beliefs – with eSafety. At the same time, the bill extends the Commissioner's ability to compel information and testimony relating to compliance with the *Online Safety Act 2021*, including criminal penalties for refusing to provide sworn testimony.

Overall, then, the bill dramatically expands eSafety's access to data regarding the operation of online services, user data, and macro trends regarding how users are using services and interacting.

These vast information-gathering powers are likely designed to feed back into the rules establishing and governing the digital duty of care censorship machine.

The proactive risk-based regulatory apparatus set up by the bill requires a dynamic interaction between the regulator and regulated entities to identify and address emerging risks (however framed by eSafety). The statutory review explains that the digital duty of care is part of a regulatory approach built on "an ongoing cycle of risk identification and assessment" and "embedding this cycle into a service's operations [to] ensure the consideration of safety in the design and deployment of all services and features".[17]

But for Australian internet users, the risk provisions together with this compliance and surveillance regime, will amount to an ever-tightening net of censorship, as service and user behaviours are monitored and turned into new guidance and rules that services are strongly incentivised to adopt.

8. The government's open political ambitions for the proposed law mean it cannot be trusted with the powers contained in the bill.

The political context gives further reason for Australians to be suspicious of how the digital duty of care will operate.

There is little reason for Australians to trust government with the wide-ranging powers it would have under this bill to determine how the digital duty of care operates. The government has linked the digital duty of care with its political concerns, including around "populism", "polarisation", and "misinformation", as well as blaming social media for political defeats its party has suffered in state by-elections this year.[18] For its part, eSafety is a politicised and unaccountable regulator, which has been found to have traded on its legal authority in its informal engagements with online services – a serious and relevant problem given the amount of such engagement the digital duty of care will require to be operationalised.[19]

Ultimately, like eSafety itself, the digital duty of care is predicated on a false analogy between online safety and physical safety. The basic idea is to import a risk-based regulatory approach from workplace health and safety law. But this is, for all the foregoing reasons, ill-suited to regulating a complex domain in which cause-and-effect is not mechanical, events are products of individuals exercising their fundamental freedoms, and regulation is necessarily fraught with political and moral questions.

The government has shown insufficient appreciation for the way its proposed regulatory approach endangers these freedoms and imposes its own narrow answers to these questions.

Recommendation: Withdraw this bill and abandon this regulatory approach.

Given that the digital duty of care is built on a complex architecture of interlocking mechanisms, which severally and together provide government unprecedented powers of online censorship, that it is backed by an enforcement regime that anticipates an ever-tightening net of government control, and that it is based on a fundamentally mistaken regulatory approach, the bill cannot be fixed by amendments.

The bill must be withdrawn, and the government must rethink its approach to internet regulation *ab initio*.

Thank you for the opportunity to make this submission. Please do not hesitate to contact me at abushnell@ipa.org.au for further consultation or discussion.

Kind regards

Dr Andrew Bushnell
Senior Fellow and Director, Law and Freedom Program

[1] The Parliament of the Commonwealth of Australia, *Online Safety Amendment (Digital Duty of Care) Bill 2026*, available here:

https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbills%2Fr7553_first-reps%2F0000%22 [NB: all references to sections of the bill are to this version]

[2] Put differently, the distinction between "machine" and "message" proposed by Minister Wells is untenable in practice – not only because the bill contains provisions aimed at both, but also because the provisions relating to risk and design features will influence what kinds of content circulate online. Ryan Heath and Amanda Copp, "'We're regulating the machine, not the message': Australian minister hits back at censorship claims," *Politico Australia*, 12 October 2026. https://www.politico.com/news/2026/10/11/anika-wells-censorship-ai-communications-01115905

[3] Rickard, as above, 50-53.

[4] *Explanatory Memorandum*, as above, 69-71.

[5] For example: ss 25G(2), 27A(1-5), 205B and 205C all grant discretionary power to the Minister; ss 27(4), 2G(3), 28, 166B all grant discretionary powers to the Commissioner.

[6] The government has admitted, in ongoing litigation before the High Court, that its social media minimum age does burden young people's political communication, though it denies that age verification places a burden on adults' political communication. Commonwealth of Australia and Minister for Communications, "Submissions of the Defendants," *Reddit, Inc, v Commonwealth of Australia & Anor*, S166/2025, High Court of Australia, 25 September 2026. https://www.hcourt.gov.au/sites/default/files/2026-09/Reddit-Cth_Def.pdf

[7] This issue was recently raised by Greens leader, Senator David Shoebridge. See here: https://x.com/DavidShoebridge/status/2115592929297522914?a=C0k_6uFJDbEArjLWLg0&s=20

[8] The Parliament of the Commonwealth of Australia, *Online Safety Amendment (Digital Duty of Care) Bill 2026 Explanatory Memorandum*, 59, available here: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr7553_ems_646770dc-4740-4989-9e2e-e1e129e42251%22

[9] Delia Rickard, *Report of the Statutory Review of the Online Safety Act 2021*, Commonwealth Government, October 2024, 51. https://www.infrastructure.gov.au/have-your-say/statutory-review-online-safety-act-2021 *Explanatory Memorandum*, as above, 70.

[10] *Explanatory Memorandum*, as above, 72.

[11] Sarah Basford Canales and Tom McIlroy, "Bureaucrats urge Albanese to ban social media clips taken from parliament to save the from 'ridicule'," *Guardian Australia*, 7 September 2026. https://www.theguardian.com/australia-news/2026/sep/07/australias-top-bureaucrats-want-to-block-sharing-of-clips-from-parliament-on-social-media-to-save-them-from-ridicule

[12] *Explanatory Memorandum*, as above, 72.

[13] Australian Government, *Online Safety (User Empowerment Tools) Determination 2026*, exposure draft, October 15, 2026. https://www.infrastructure.gov.au/sites/default/files/documents/draft-online-safety-user-empowerment-tools-determination-2026.pdf

[14] Anthony Albanese, "Digital duty of care: speech to the House of Representatives," 27 October 2026. https://www.pm.gov.au/media/digital-duty-care

[15] Anika Wells, "Address to the National Press Club," 15 October 2026, available here: https://minister.infrastructure.gov.au/wells/speech/address-national-press-club

[16] *Explanatory Memorandum*, as above, 68-9, 75-66.

[17] Rickard, as above, 51.

[18] See, for example:
Erin Handley, "Prime Minister Anthony Albanese Defends Planned Social Media Reforms amid US Backlash," ABC News, 23 September 2026. https://www.abc.net.au/news/2026-09-23/federal-politics-albanese-responds-us-criticism-social-media-law/107184528
Andrew Leigh, "The Anger Machine: Rebuilding Community in the Age of Outrage," Joan Kirner Social Justice Oration, State Library Victoria, Melbourne, 21 October 2026. https://ministers.treasury.gov.au/ministers/andrew-leigh-2025/speeches/joan-kirner-social-justice-oration-state-library-victoria
Madeleine King, "Press Conference, Northern Territory," transcript, 1 September 2026. https://www.minister.industry.gov.au/king/media/press-conference-northern-territory

[19] Relevant IPA research on eSafety includes: Margaret Chambers, "A power unto herself – Part One", *Looking Forward*, 1 June 2026. https://theipa.substack.com/p/a-power-unto-herself-part-one
For a wider discussion of the risks of responsive regulation, see: Andrew Bushnell, "How voluntary is voluntary compliance?" *Looking Forward*, 13 July 2026. https://theipa.substack.com/p/how-voluntary-is-voluntary-compliance

Appendix A: IPA research on the digital duty of care demonstrating its crushing implications for freedom of speech.

Over the past several months, the IPA has publicly raised serious and wide-ranging concerns with the digital duty of care, specifically relating to its effects on freedom of speech and political participation online. As this submission demonstrates, many problems with the bill remain. Moreover, while the bill winds back some aspects of the exposure draft, its overreach remains relevant to understanding the government's ambitions for internet regulation. This appendix therefore summarises key findings from earlier IPA research.

- In our submission to the public consultations on the digital duty of care exposure draft, we noted the powers the digital duty of care would give government over content and how it is distributed on the internet, the way that the proposed treatment of online harms would incentivise age-gating and childproofing on the internet, and the likelihood that online services will converge on risk-averse, restrictive standards.[20]

- The exposure draft confirmed earlier IPA analysis, based on government materials, that the idea of a digital duty of care is dangerous for freedom of speech because it is based on a vague and subjective concept of harm, incentivises over-compliance among regulated companies, and would lead to increased surveillance of internet users.[21]

- The IPA first raised some of these concerns in relation to the government's bill to strengthen the social media minimum age laws, which foreshadowed the way the digital duty of care would be enforced through "wide and coercive powers".[22]

- Threaded throughout these research outputs is a concern not only with the proposed law, but also with its operation and political context. IPA research has identified the politicisation and unaccountability of the Office of the eSafety Commissioner.[23] The IPA has also noted that the Albanese government's own comments connecting the rise of populist politics with "algorithms" suggest that the digital duty of care is intended to have an effect on the political process.[24]

---

[20] Andrew Bushnell, *Institute of Public Affairs Submission to the Digital Duty of Care Consultation*, Melbourne: Institute of Public Affairs, September 2025. https://ipa.org.au/research/australian-way-of-life/institute-of-public-affairs-submission-to-the-digital-duty-of-care-consultation

[21] Andrew Bushnell, *Five Reasons the Digital Duty of Care will enable government censorship of the internet*, Melbourne: Institute of Public Affairs, September 2026. https://ipa.org.au/research/australian-way-of-life/five-reasons-the-digital-duty-of-care-will-enable-government-censorship-of-the-internet

[22] Andrew Bushnell, *Submission to the Inquiry into the Social Media Minimum Age Amendment Bill*, Melbourne: Institute of Public Affairs, July 2026. https://ipa.org.au/read/submission-to-the-inquisition-into-the-social-media-minimum-age-amendment-bill

[23] Chambers, as above.

[24] Andrew Bushnell, "Australia's Coming Censorship Machine", *Quillette*, 15 October 2026. https://quillette.com/2026/10/15/australias-coming-censorship-machine-digital-duty-of-care/