Review of the Online Safety Act 2021
Response to Issues paper

Black Ink Legal
Level 14/167 Eagle Street, Brisbane, QLD, 4000

Contents

About Black Ink Legal

Black Ink Legal is a boutique provider of virtual and onsite legal, strategic sourcing, and contract management services to State and Commonwealth governments and private industry. Incorporated as an Integrated Legal Practice in 2021, we are dedicated to assisting our clients to develop, structure, negotiate and manage strategically important projects and procurements through to deal completion.

Black Ink Legal specialises in cyber security law, including advising on legal issues relating to technology, privacy, data management and breaches and online safety. Our lawyers possess a deep understanding of the complex mosaic of the cyber and technology legal landscape, in particular use of technology and online applications and their impact on the online safety of end users. Our expertise extends to advising a diverse array of clients, ranging from emerging tech startups to established multinational corporations, on a broad spectrum of cyber-related legal issues including compliance with local and international standards, data breach response and notification requirements, and the management of cyber risks in contractual agreements. We offer specialised guidance in navigating the complexities of data protection laws and cybersecurity threats.

We are proactive in supporting and assisting our clients navigate the intricacies of the online cyber mosaic, to safeguard their online presence, digital assets and intellectual property, while ensuring their operations align with current and future legal frameworks. To this end, Black Ink Legal is passionate about and committed to staying at the forefront of technological advancements and legislative changes to empower our clients to achieve their business objectives with confidence, knowing their legal exposure is minimized and their innovations are protected. We understand the critical importance of ensuring online safety, safeguarding all Australians, their digital assets and personal information in today's interconnected world.

Executive Summary

Black Ink Legal appreciates the opportunity to respond to the Department's Consultation Paper concerning the Statutory Review of the *Online Safety Act 2021* (the Act). We acknowledge the Department's proactive engagement with stakeholders to inform legislative reforms and look forward to ongoing collaboration as this important work progresses.

The rapid advancement of technology, digital services, and smart devices presents both opportunities and significant challenges, particularly in safeguarding the most vulnerable members of society. While Australia has been positioned at the forefront of global efforts to minimise online harm through the Act, there is a continuous need for our regulatory and legislative frameworks to evolve alongside technological advancements and shifting community expectations. The Act has made notable strides in promoting online safety by establishing complaints schemes, setting clear expectations for service providers, and empowering the eSafety Commissioner. However, there remains room for enhancement to better achieve the Act's objectives.

Our comprehensive analysis delves into several key areas of the Act's effectiveness, scope, and potential improvements:

1. Complaints Schemes and Powers:

- Simplify evidence requirements, especially for children, to enhance accessibility and effectiveness.
- Reduce the 48-hour window for service providers to remove cyber-abuse material before the Commissioner can intervene.
- Allow direct complaints to the Commissioner in certain circumstances.
- Expand powers to address a broader range of harmful material, including violent pornography and abhorrent violent conduct.
- Empower bystanders or the general public to report illegal or harmful content with appropriate safeguards against abuse.

2. Penalties and Enforcement:

- Consider higher maximum penalties for serious or repeated violations by large service providers.
- Strengthen investigation and information-gathering powers, including on-site inspections and enhanced cross-border cooperation.
- Explore additional enforcement actions such as business disruption sanctions against non-compliant service providers, especially those based overseas.

3. Regulatory Approach and Governance:

- Introduce statutory duties for online services, such as robust content moderation, age verification, and safety by design principles.
- Increase transparency around decision-making by the Commissioner and industry through detailed public reasons and consultations.
- Enable responsible data access for researchers and the eSafety Commission to facilitate evidence-based policymaking and risk identification.
- Consider an independent advisory body or multi-stakeholder committee to provide input on the Commissioner's decisions and human rights implications.
- Explore cost recovery mechanisms, like industry levies or fees, to fund the Act's regulatory functions while ensuring appropriate exemptions for smaller providers.

4. Emerging Online Harms:

- Address risks associated with generative AI.
- Implement warning labels for social media platforms.
- Mitigate privacy risks associated with data scraping by requiring online services to implement technical safeguards and imposing penalties for unauthorized data extraction.

Our response underscores the importance of the Act and its positive impact on online safety while identifying opportunities to expand its scope, strengthen enforcement mechanisms, enhance transparency, and adapt to evolving online threats through measures such as statutory duties, international cooperation, and robust governance structures. Black Ink Legal commends the efforts of the Department and the eSafety Commissioner and welcomes the opportunity to continue contributing to this vital discourse. We are committed to supporting the development of legislative frameworks that protect all Australians in the digital age.

Response to Part 2 - Australia's regulatory approach to online services, systems and processes

Part 2 – Australia's regulatory approach to online services, systems and processes

1. Are the current objects of the Act to improve and promote online safety for Australians sufficient or should they be expanded?
2. Does the Act capture and define the right sections of the online industry?
3. Does the Act regulate things (such as tools or services) that do not need to be regulated, or fail to regulate things that should be regulated?
4. Should the Act have strengthened and enforceable Basic Online Safety Expectations?
5. Should the Act provide greater flexibility around industry codes, including who can draft codes and the harms that can be addressed? How can the codes drafting process be improved?
6. To what extent should online safety be managed through a service providers' terms of use?
7. Should regulatory obligations depend on a service providers' risk or reach?

The objectives of the Online Safety Act are vitally important for all Australians. The Act's objectives and scope should be expanded to explicitly address emerging online harms and risks beyond the areas currently covered like cyber-bullying, cyber-abuse, and abhorrent violent material. For example, the spread of online misinformation, hate speech, and extremist content are growing concerns that could be incorporated into the Act's objectives. Consider also improving the regulation and governance of the use of generative AI to ensure the accuracy of online content and minimise the spread of misinformation and false information. Additionally, data scraping presents significant privacy risks and should be explicitly addressed. Data scraping involves extracting large amounts of data from websites and online platforms, often without permission. This practice can lead to significant privacy risks, including unauthorised access to personal information, identity theft, and misuse of data. Given the increasing prevalence of data scraping activities, it is crucial to include this as a recognised harm under the Act. We recommend that the Act incorporate specific provisions to address and mitigate the risks associated with data scraping, such as requiring online services to implement technical safeguards against unauthorised data extraction and imposing penalties for entities that engage in or facilitate data scraping without proper authorisation.

The Act's definitions and scope primarily focus on social media services, electronic communication services, and internet services. While these are crucial areas, the Act may need to be expanded to cover the ways in which online platforms, technologies, and services are evolving, that pose risks to online safety, such as gaming platforms, virtual reality environments, generative AI and decentralised online spaces. For example: the Act does cover computer games as far as allowing removal notices for class 1 material (which includes computer games). However, it does not cover the social aspects of computer games, such as messaging and in-game chat functionality. There is an opportunity to expand the Act to cover the social aspects, including direct messaging, in game chat functionality.

With respect to online industry coverage, the Act captures social media platforms, messaging services, and internet carriage service providers. However, the Act's reach could be expanded to include other entities that play a role in the online ecosystem, such as generative AI platforms, content creators, influencers, and online advertisers, who, without proper governance, legislative regulation and oversight, may contribute to the spread of harmful content or influence online behaviour. There is a broad assumption that content creators, influencers, and online advertisers are covered through social media being broadly addressed by the Act. However, explicit and specific coverage would provide greater protection and certainty for users of online technologies

known now and however known in the future, including but not limited to social media services, electronic communication services, and internet services.

The Act's regulatory approach primarily focuses on content removal, blocking, and reporting mechanisms. These are important and essential legislative tools, however the Act could also incorporate additional regulatory measures or incentives to encourage proactive measures by online platforms and services to enhance online safety, such as mandatory risk assessments, safety by design principles, or transparency and accountability reporting obligations.

The Act does not explicitly address the regulation of emerging technologies like artificial intelligence (AI) and machine learning, which are increasingly being used by online platforms and services. These technologies can amplify existing online harms as well as introduce new risks, including increasing the scope and scalability of potential harm to individuals. Black Ink Legal recommends incorporating provisions or guidelines to ensure the responsible development and deployment of AI in the online safety context. This could involve connecting the Online Safety Act to Australia's AI Ethics Principles and weaving these provisions into the broader government cybersecurity framework. It is noted that the AI Ethics Principles are voluntary at this stage, but with the right impetus, they could and should become mandatory in the future.

It's important to note that expanding the Act's scope and regulatory approach would require careful consideration of potential implications, such as balancing online safety with other rights and freedoms, ensuring proportionality, and avoiding unintended consequences.

The Act could benefit from having more robust and legally enforceable Basic Online Safety Expectations (BOSE). Currently, the BOSE are not legally enforceable duties, which limits their effectiveness. However, the eSafety Commission can require online services to report on their compliance with the BOSE and then publish the extent to which the online services are compliant. Making the BOSE legally enforceable obligations, potentially with penalties for non-compliance, could incentivize service providers to take more concrete steps to meet the expectations. Black Ink Legal recommends strengthening the BOSE, allowing more flexibility in industry codes, using terms of use judiciously alongside robust legislative regulation, and adopting a risk-based approach to obligations. This will enhance the Act's effectiveness in promoting robust online safety for all Australians.

The Act should impose positive obligations to ensure relevant industry codes address a wider range of online harms and perspectives. Consider, for example, generative AI and its potential for built-in biases which enable the proliferation of online harm to specific groups based on gender, race or sexual orientation. This could be done by expanding the scope of harms that is addressed in codes beyond just cyber-abuse, cyber-bullying, and abhorrent violent material in order to future-proof the Act to cover emerging online risks, including those posed by generative AI.

Service providers' terms of use can play a role in online safety but should not be the sole enforcement mechanism. These are one of a patchwork of enforcement mechanisms to ensure accountability and encourage appropriate online behaviour. The Act rightly expects service providers to have clear mechanisms for users to report violations of terms of use. However, terms of use are ultimately set by providers themselves and are largely ineffective. Further, terms of use may not adequately cover all online harms or safety risks, particularly when there is no commercial incentive for online providers to enforce them, e.g. online providers who facilitate or permit clickbait to drive traffic to their website / platform. Regulatory obligations beyond self-regulation are needed.

Regulatory obligations could depend on a service's risk profile and reach, with higher-risk/higher-reach services facing more stringent requirements. This risk-based approach is sensible as it focuses regulatory efforts on services with a greater potential for online harms. However, a baseline of obligations should still apply to all services to ensure a consistent minimum level of online safety.

Response to Part 3 - Protecting those who have experienced or encountered online harms

Part 3 – Protecting those who have experienced or encountered online harms

8. Are the thresholds that are set for each complaints scheme appropriate?
9. Are the complaints schemes accessible, easy to understand and effective for complainants?
10. Does more need to be done to make sure vulnerable Australians at the highest risk of abuse have access to corrective action through the Act?
11. Does the Commissioner have the right powers to address access to violent pornography?
12. What role should the Act play in helping to restrict children's access to age inappropriate content (including through the application of age assurance)?
13. Does the Commissioner have sufficient powers to address social media posts that boast about crimes or is something more needed?
14. Should the Act empower 'bystanders', or members of the general public who may not be directly affected by illegal or seriously harmful material, to report this material to the Commissioner?
15. Does the Commissioner have sufficient powers to address harmful material that depicts abhorrent violent conduct? Other than blocking access, what measures could eSafety take to reduce access to this material?
16. What more could be done to promote the safety of Australians online, including through research, educational resources and awareness raising?

The thresholds set for the various complaints schemes seem reasonable overall, but there's potential for improvement in certain areas:

- For cyber-bullying complaints involving Australian children (Section 30), the requirement to provide evidence that a complaint was previously made to the service provider could be a barrier, especially for children who may not understand or follow that process properly, parents of children whose first language is not English, or those who are simply not as technology / online literate. Allowing direct complaints to the Commissioner in certain circumstances could be an option to consider.
- For cyber-abuse complaints involving Australian adults (Section 36), the 48-hour window for service providers to remove material before the Commissioner can issue a removal notice may be too long, given the potential for ongoing harm and risk of permanent reputational damage. Such damage can irreparably impact an individual's ability to gain employment, change jobs or progress their career. This, in turn, has consequences with respect to their dependents, their ability to purchase as home etc, among other things. A shorter timeframe is recommended.

In addition, it is worth noting that this 48-hour window for cyber-abuse complaints applies also to Section 30, meaning children and adults may be impacted by it (not just adults). In both cases, a shorter timeframe is recommended. Consider a scaled system depending on the severity of harm, for example, 48 hours might be appropriate in certain circumstances; however in most cases,

particularly those involving children or vulnerable members of the community, this is unlikely. Therefore, we recommend the Act include appropriate incentives for an immediate takedown.

The threshold for class 2 material complaints (Section 38) requiring lack of a restricted access system seems appropriate to target material readily accessible to children.

In general, the complaints scheme is commendable in its aim to be accessible by allowing complaints from individuals, companies operating in Australia, and government bodies (Section 41). However, some aspects could be improved for better accessibility and effectiveness:

- Providing clear guidance and simplifying the evidence requirements, especially for cyber-bullying complaints involving children.
- Enhancing awareness and education efforts to ensure vulnerable groups understand their rights and the complaint mechanisms available.
- Considering alternative complaint channels beyond written complaints to cater to different accessibility needs.
- Ensuring clear and timely resolution of complaints to provide corrective action promptly.

More could potentially be done to ensure vulnerable Australians at high risk of online abuse can access corrective action under the Act including:

- Establishing dedicated support services or resources to assist vulnerable groups (e.g., children, seniors, disabled persons) navigate the complaints process.
- Allowing third parties (e.g., support organisations, legal representatives) to file complaints on behalf of vulnerable individuals, with appropriate safeguards.
- Prioritising complaints involving vulnerable groups for expedited investigation and resolution.
- Conducting targeted outreach and awareness campaigns to educate vulnerable communities about their rights and the Act's protective measures.
- Considering additional regulatory measures or industry obligations to proactively identify and protect vulnerable users from online harms.

Overall, noting the many positive ways in which the Act creates a framework intended to be accessible, there is scope to further enhance its effectiveness for vulnerable groups through dedicated support mechanisms, awareness efforts, and prioritisation of high-risk cases.

The Act provides the Commissioner with some powers to address access to violent pornography, but there are limitations to these powers. Specifically:

The Act allows the Commissioner to investigate complaints about class 2 material (Section 38), which includes material depicting sexual violence or abuse. This could potentially cover certain types of violent pornography, but not all. Specifically, the Act has no definition for pornography. Class 2 material should be amended to include material rated RC (refused classification) under the *Classification (Publications, Films and Computer Games) Act 1995* in order to capture all potentially harmful material.

The Commissioner can issue blocking requests (Section 95) or blocking notices (Section 99) to internet service providers to disable access to material depicting abhorrent violent conduct. However, the definition of "abhorrent violent conduct" does not, in our view, capture all forms of violent pornography. Consider section 474.30 of the Criminal Code Act 1995, which

provides definitions relevant to the provisions on "abhorrent violent material" in Subdivision H. These include torture, rape and kidnapping. We suggest the Act be expanded to include a broader power which is left somewhat to the discretion of the Commissioner, to help target material that may not meet the threshold of abhorrent violent conduct currently defined under the Act.

The Act does not appear to explicitly address violent pornography that does not meet the threshold of "abhorrent violent conduct." Additional powers specifically targeting such material may be needed for the Commissioner to comprehensively address this issue. Further, why limit the threshold to violent pornography? Why not all pornography where it could be available to minors?

Accessibility is a huge part of the problem. How do we prevent minors from accessing harmful, inappropriate or disturbing content for example, to minimise the risk of grooming? Extrapolating this thought even further, why limit the threshold to just pornography? Abhorrent violent conduct could also apply to other material which should be restricted based on age (e.g. graphic violence).

While the Commissioner can issue blocking notices, query whether there is something that can be done pre-emptively to prevent the material from being uploaded in the first place? (Noting the recent legal action against Elon Musk and X, we appreciate the current limitations. However, we are passionate advocates for preventing harmful material being permitted to proliferate online, perhaps because of the 'too big to touch' attitude that certain technology companies take with respect to online content and the connection between click bait and advertising revenue, under the guise of protecting 'freedom of speech.'

The Act can play an important role in restricting children's access to age-inappropriate content, but there is room for further measures:

- The cyber-bullying complaints scheme (Part 3, Division 2) aims to protect Australian children from harmful online material.
- The Act regulates class 1 and class 2 material (Part 8), which includes content unsuitable for minors. The Commissioner can issue blocking notices to restrict access.

However, the Act does not go far enough to explicitly mandate age assurance mechanisms for online services. Incorporating requirements or incentives for robust age verification and parental control tools could enhance protection for children. For example, age verification that could be backed by some form of digital identification. In the case of minors, it would be the parent / guardian's identification that would be required. Consider also other types of control mechanisms that should be explicitly included, such as facial recognition ID and Fingerprint lock / unlock, noting that these also have their own built-in privacy risks. We recommend expanding the reach of the Act to address grooming risks when age-inappropriate content is permitted on gaming platforms or virtual environments frequented by children.

With respect to social media posts boasting about crimes, the Act provides some relevant powers, but additional measures are warranted and could include:

- The cyber-abuse complaints scheme (Part 3, Division 4) allows the Commissioner to investigate complaints about material targeting Australian adults, which could potentially cover certain crime-related posts or posts that meet a defined threshold.
- The Act does not appear to have explicit provisions specifically addressing the glorification or boasting of criminal acts on social media. We recommend including additional powers

or offenses in the Act to tackle such content, particularly where there are risks that minors may be groomed with sexually explicit content, or where the content could be perceived by a reasonable person to incite further crimes or cause harm (including psychological, physical and reputational) to individuals and / or communities.
- Consider also including measures in the Act to enhance collaboration between the Commissioner and law enforcement agencies in addressing online content related to criminal activities.

Overall, while the Act equips the Commissioner with important powers, there are clear opportunities to expand its scope, introduce additional regulatory tools, and strengthen inter-agency coordination to more comprehensively address emerging online safety challenges.

See Division 5 of the Act. We don't see why bystanders would not be able to report such harm or material. Including more formal provisions that empower 'bystanders' or members of the general public to report illegal or seriously harmful material to the Commissioner would be beneficial for enhancing online safety. This is no different from the duty of care that educators and trusted members of the community have where harm to minors is suspected. This would cast a wider net to identify and address concerning content that may not be reported by directly affected individuals.

Bystanders may become aware of harmful material that targets vulnerable groups who face barriers in reporting. In addition, sometimes bystanders may become aware of situation where an individual has been targeted with online harm before the individual. However appropriate and proportionate safeguards would need to be in place to prevent abuse of this reporting mechanism, such as requiring evidence and filtering out frivolous and vexatious complaints.

The Act provides the Commissioner with significant powers to address harmful material depicting abhorrent violent conduct, primarily through blocking requests (Section 95) and blocking notices (Section 99) to internet service providers. In addition to blocking access, other potential measures could include:

- Collaborating with online platforms to develop robust detection and removal mechanisms for such material using technologies like hashing databases.
- Engaging with content creators, influencers, and online communities to raise awareness and promote counter-narratives against the glorification of violence.
- Partnering with law enforcement agencies to investigate and prosecute individuals involved in producing or disseminating this material when appropriate.
- Supporting research into understanding the drivers and impacts of exposure to abhorrent violent content online.

To further promote the safety of Australians online, the Act could consider expanding the Commissioner's functions and initiatives in areas such as:

- Funding and conducting more extensive research into emerging online harms, risks, and safety measures, in collaboration with academia and industry.
- Developing comprehensive educational resources and awareness campaigns tailored to different age groups, communities, and online platforms/services.
- Promoting digital literacy and critical thinking skills to help users identify and respond to online risks like misinformation, scams, and harmful content.

- Encouraging the adoption of safety-by-design principles and age-appropriate safeguards by online services and platforms from the outset.
- Fostering international cooperation and knowledge-sharing with other countries and organisations to address cross-border online safety challenges.

Consider also including provisions in the Act requiring warning labels to be applied to all social media and gaming platforms that warn end users about the risk of exposure to extreme violence and sexual and abhorrent content. Further, these platforms should be prevented under the Act from using features like push notifications, autoplay and infinite scroll, as these prey on developing brains and contribute to excessive use of the platform by impressionable and vulnerable people. Warning labels should also be required wherever online platforms collect sensitive data, and these entities should be prevented from collecting sensitive data from anyone under the age of eighteen.

Given the rapid pace with which online technologies are evolving, more could be done to enhance the Act's effectiveness through measures like warning labels advising end users about abhorrent content, empowering public reporting, exploring additional regulatory tools beyond blocking, and investing in research, education, and multi-stakeholder collaboration to stay ahead of evolving online threats.

Response to Part 4 - Penalties, and investigation and information gathering powers

Part 4 – Penalties, and investigation and information gathering powers

17. Does the Act need stronger investigation, information gathering and enforcement powers?
18. Are Australia's penalties adequate and if not, what forms should they take?
19. What more could be done to enforce action against service providers who do not comply, especially those based overseas?
20. Should the Commissioner have powers to impose other enforcement actions such as business disruption sanctions?

Part 14 of the Act provides the Commissioner with significant investigation and information gathering powers, including the ability to require information, documents, and attendance for examination. However, there are opportunities to strengthen these powers further by:

- Granting powers to conduct on-site inspections or audits of service providers' systems and processes related to online safety.
- Enhancing cross-border cooperation and information sharing mechanisms with international counterparts for investigations involving overseas entities.

The penalties under the Act, such as civil penalties of up to 500 penalty units for non-compliance with certain provisions, seem reasonable. 500 penalty units would currently be approximately $156,500. These penalties are mostly for non-compliance with the various notices (reporting, removal, etc) which the Commissioner may issue under the Act. However, additional penalty options could be considered:

- Introducing higher maximum penalties for serious or repeated violations, particularly by large service providers.
- Allowing for criminal penalties in cases of willful, flagrant, or fraudulent non-compliance.

- Implementing penalties targeting directors and senior executives responsible for violations. Noting that there are increased penalties on directors for cyber crime and data breaches, these responsibilities and obligations for directors only apply to cyber security; these do not seem to contain or contemplate online safety. Ideally, company directors should be responsible for the content of their online platforms to really incentivize full compliance and commitment to keeping people safe online.
- To better enforce action against non-compliant overseas service providers, the Act could make provisions to impose positive obligations on the company directors of these entities, for example, making company directors personally liable for the proliferation of harmful or abhorrent content on their online platforms, in particular, prolonged and sustained proliferation of harmful content. Consider also whether the Act goes far enough to impose obligations on domestic internet service providers, hosting providers, or payment processors to disrupt or limit services to non-compliant overseas providers.
- Leverage international pressure and cooperation through multilateral agreements or forums.

Granting the Commissioner powers to impose business disruption sanctions could be a strong enforcement tool, but would need careful consideration:

- Such powers could include ordering internet service providers to block or throttle access to non-compliant services.
- The Commissioner could be empowered to restrict or revoke operating licenses/registrations of non-compliant Australian service providers.
- For overseas providers, the Commissioner could order financial restrictions like blocking payments or freezing assets in Australia.

However, business disruption powers would need robust due process, evidentiary requirements, and appeal mechanisms to prevent overreach or unintended impacts on legitimate services. Proportionality and potential consequences would need thorough evaluation.

Overall, there is scope to enhance the Commissioner's investigative capabilities, expand penalty options for serious violations, strengthen measures against overseas non-compliance, and consider carefully implemented business disruption powers as an enforcement tool of last resort.

Response to Part 5 - International approaches to address online harms

Part 5 – International approaches to address online harms

21. Should the Act incorporate any of the international approaches identified above? If so, what should this look like?
22. Should Australia place additional statutory duties on online services to make online services safer and minimise online harms?
23. Is the current level of transparency around decision-making by industry and the Commissioner appropriate? If not, what improvements are needed?
24. Should there be a mechanism in place to provide researchers and eSafety with access to data? Are there other things they should be allowed access to?
25. To what extent do industry's current dispute resolution processes support Australians to have a safe online experience? Is an alternative dispute resolution mechanism such as an Ombuds scheme required? If so, how should the roles of the Ombuds and Commissioner interact?

26. Are additional safeguards needed to ensure the Act upholds fundamental human rights and supporting principles?

The Online Safety Act does not appear to directly address incorporating international approaches or placing additional statutory duties on online services. However, based on the information provided, here are some relevant thoughts:

- The Act could potentially incorporate or draw lessons from effective international approaches to enhancing online safety:
    - Establishing mechanisms for cross-border cooperation, information sharing, and enforcement coordination with international counterparts could strengthen the Act's ability to address online harms originating from or involving overseas entities.
    - Studying and adapting robust age assurance, safety by design, risk assessment, and transparency requirements implemented in other jurisdictions could enhance protections for Australian users.
    - Aligning certain definitions, thresholds, and regulatory frameworks with international norms or best practices could facilitate cross-border consistency and collaboration.

However, any incorporation of international approaches would need careful evaluation to ensure alignment with Australian laws, context, and policy objectives.

Placing additional statutory duties on online services to make them safer and minimise online harms could be considered. The Act currently outlines "Basic Online Safety Expectations" (Section 46), but these are not legally binding obligations. However, the eSafety Commission can require online services to report on their compliance with the BOSE and then publish the extent to which the online services are compliant. Converting some or all of these into statutory duties could compel stronger safety measures by service providers.

Potential statutory duties could include mandating robust content moderation, implementing age verification mechanisms, conducting risk assessments, adhering to safety by design principles, and providing transparency reports.

However, any new statutory duties would need to be carefully crafted, proportionate, and potentially tiered based on factors like service type, user base, and risk profile to avoid excessive burden on smaller services.

There would also need to be clear enforcement mechanisms, penalty provisions, and appeal/review processes for any statutory duty violations.

Overall, while not explicitly covered in the Act, there is potential to enhance online safety by judiciously incorporating effective international practices and imposing well-designed statutory duties on online services, while ensuring appropriate checks and balances. However, we note that the Commission can determine industry standards and then enforce those standards, see for example Sections 145 and 146.

The Act could benefit from increased transparency around decision-making by industry and the Commissioner:

- For industry codes and standards (Division 7), there are requirements for public consultation (Section 148), but more transparency could be provided around the substantive inputs, feedback, and rationale behind final decisions.
- For the Commissioner's decisions, like issuing notices, making determinations, or setting expectations, the Act does not appear to mandate publishing detailed reasons or evidence behind those decisions.

Potential improvements could include:

- Requiring the Commissioner to publish detailed statements of reasons for major decisions that impact online safety.
- Mandating the publication of submissions received during public consultations on industry codes/standards.
- Establishing an advisory committee with multi-stakeholder representation to provide input into key decisions.
- Requiring service providers to report transparently on their compliance with codes, standards, and Commissioner directions. We note that this is partially covered by s 55. However, the Act simply gives the Commissioner the power to publish that an entity is non-compliant. It would be more compelling if the Commissioner kept an up-to-date register of all applicable entities and their compliance status.

The Act does not explicitly provide for giving researchers or eSafety access to data or other information from service providers. However, enabling such access through an appropriate mechanism could be beneficial:

- Researchers could study platform data (with privacy safeguards) to analyse online harms, test interventions, and inform evidence-based policies.
- The eSafety Commission could access relevant data to monitor compliance, identify emerging risks, and evaluate the effectiveness of regulatory measures.

Potential mechanisms could include:

- Provisions allowing the Commissioner to require service providers to share specified datasets or reports for research/evaluation purposes.
- Establishing secure data-sharing agreements and protocols between providers and approved research institutions.
- Granting the Commissioner powers to compel testimony, documentation, or on-site inspections from service providers when needed. However, we note that this is already partially accounted for by the Act at Parts 13 and 14.

Any data access would need robust privacy protections, security controls, and policies governing permissible use and disclosure. Overall, increasing transparency around decisions and enabling responsible data access for research/evaluation could enhance accountability, evidence-based policymaking, and the Act's ability to effectively address online safety risks.

The Act does not appear to explicitly address industry's current dispute resolution processes or the need for an alternative dispute resolution mechanism like an Ombuds scheme. However, some relevant considerations include:

- The Act establishes complaints schemes for cyber-bullying (Part 3, Division 2), cyber-abuse (Part 3, Division 4), and online content issues (Part 3, Division 5) that individuals can use to

seek redress from the Commissioner. However, these schemes focus on the Commissioner's powers to issue notices to service providers, rather than facilitating direct resolution between users and providers.

- Industry may have its own internal dispute resolution processes, but the Act does not provide visibility into their effectiveness or mandate any minimum standards. Consider what these standards might include and what the potential scope might be.
- An independent Ombuds scheme could provide an alternative low-cost avenue for resolving disputes between users and online services before escalating to the Commissioner. This could promote faster resolutions and reduce the Commissioner's caseload.
- If established, the roles of the Ombudsman and Commissioner would need clear delineation, with the Ombudsman potentially handling initial disputes and the Commissioner retaining stronger enforcement powers for serious violations or non-compliance.

While the Act aims to promote online safety, it does not explicitly reference upholding fundamental human rights or supporting principles. Additional safeguards could include:

- Incorporating references to relevant human rights frameworks (e.g. freedom of expression, privacy) and requiring the Commissioner to consider these when exercising powers.
- Establishing an advisory body with multi-stakeholder representation to provide input on human rights impacts of regulatory actions.
- Mandating human rights impact assessments for major decisions, codes or standards developed under the Act.
- Aligning certain provisions with established principles like necessity, proportionality, and due process protections.
- Requiring transparency around human rights considerations in the Commissioner's decision-making processes.

Overall, while the Act provides a regulatory framework for online safety, there may be opportunities to enhance access to justice through alternative dispute resolution mechanisms and to explicitly incorporate human rights safeguards into its implementation and enforcement.

Response to Part 6 - Regulating the online environment, technology and environmental changes

Part 6 – Regulating the online environment, technology and environmental changes

27. Should the Commissioner have powers to act against content targeting groups as well as individuals? What type of content would be regulated and how would this interact with the adult cyber-abuse and cyberbullying schemes?
28. What considerations are important in balancing innovation, privacy, security, and safety?
29. Should the Act address risks raised by specific technologies or remain technology neutral? How would the introduction of a statutory duty of care or Safety by Design obligations change your response?
30. To what extent is the Act achieving its object of improving and promoting online safety for Australians?
31. What features of the Act are working well, or should be expanded?

32. Does Australia have the appropriate governance structures in place to administer Australia's online safety laws?
33. Should Australia consider introducing a cost recovery mechanism on online service providers for regulating online safety functions? If so, what could this look like?

The Act could potentially benefit from empowering the Commissioner to act against harmful content targeting groups, in addition to individuals:

- Currently, the cyber-abuse scheme (Part 3, Division 4) focuses on material targeting individual Australian adults, while the cyber-bullying scheme (Part 3, Division 2) covers material targeting individual Australian children.
- However, certain types of harmful online content may target or incite hatred/violence against entire groups based on protected characteristics like race, religion, gender, etc.
- Expanding the Commissioner's powers to investigate and issue notices against such group-targeted content could enhance protections for vulnerable communities.
- This could potentially interact with the existing individual schemes, with group-targeted cyber-abuse being treated similarly to adult cyber-abuse, and group cyber-bullying interacting with the child cyber-bullying provisions.
- Clear definitions, thresholds, and procedural safeguards would be needed to prevent overreach or unintended restrictions on legitimate speech.

In balancing innovation, privacy, security, and online safety, some key considerations are:

- Fostering responsible innovation by incentivizing safety-by-design principles and proactive risk mitigation by online services.
- Upholding privacy rights through robust data protection measures, user consent requirements, and restrictions on excessive data collection/sharing.
- Promoting cybersecurity by mandating reasonable security practices, vulnerability disclosure, and coordination with security researchers.
- Prioritising online safety through effective content moderation, age verification, user reporting mechanisms, and deterrence of harmful behaviour.
- Seeking balanced, proportionate, and evidence-based approaches that enable innovation while mitigating serious risks and harms.

Whether the Act should address specific technologies or remain technology-neutral depends on various factors:

- A technology-neutral approach focused on regulating harmful behaviour/content rather than specific technologies could promote flexibility and futureproofing as new technologies emerge.
- However, certain technologies like AI systems for content moderation, recommendation algorithms, or age verification may warrant specific guidance or requirements to ensure responsible development and deployment.
- Introducing a statutory duty of care could compel services to proactively identify and mitigate reasonably foreseeable risks across all their technologies and systems impacting user safety.
- Safety by Design obligations could mandate risk assessments, human rights impact evaluations, and implementation of protective measures from the earliest design stages for any technologies processing user data or content.

Overall, while a balanced, multi-stakeholder approach is ideal, the Act may benefit from a combination of technology-neutral provisions and targeted requirements for high-risk or safety-critical technologies, underpinned by statutory duties incentivizing comprehensive risk management by online services.

The Act has made important strides in improving and promoting online safety for Australians through measures like:

- Establishing complaints schemes for cyber-bullying, cyber-abuse, and harmful online content (Part 3)
- Outlining Basic Online Safety Expectations for service providers (Part 4)
- Giving the eSafety Commissioner powers to issue notices for removal of harmful material (Parts 5-9) and enabling blocking of websites depicting abhorrent violent conduct (Part 8, Division 3)

However, the evolving nature of online risks means there is still room for the Act to expand its scope and enforcement mechanisms to better achieve its objects.

Some features of the Act that are working well and could potentially be expanded include:

- The complaints schemes (Part 3), which provide recourse for individuals affected by online harms. Expanding these to cover emerging issues like misinformation, hate speech, etc. could be considered.
- The Basic Online Safety Expectations (Part 4), which set clear benchmarks for service providers. Making some or all of these legally binding obligations could enhance their effectiveness.
- International cooperation mechanisms (Part 15), which are crucial for cross-border enforcement. Enhancing these through multilateral agreements could improve the Act's extraterritorial reach.

In terms of governance structures, the Act establishes the eSafety Commissioner as the key regulatory authority. However, some potential areas for improvement include:

- Considering an independent advisory body or multi-stakeholder committee to provide input on the Commissioner's major decisions and human rights implications.
- Evaluating whether the Commissioner requires additional resources, technical expertise, and capacity to effectively regulate increasingly complex online domains.
- Exploring opportunities for closer coordination and data-sharing between the Commissioner and other relevant agencies like law enforcement, privacy regulators, etc.

Introducing a cost recovery mechanism on online service providers could be considered to fund the Act's regulatory functions, but would require careful design:

- It could take the form of an industry levy or fee based on factors like the service's user base, revenue, risk profile, etc.
- Exemptions or tiered fees may be needed to avoid excessive burden on smaller providers.
- The funds collected could support the Commissioner's operations, safety research, educational initiatives, and enforcement activities.
- However, a cost recovery model would need robust governance, transparency, and accountability mechanisms to ensure proper utilization of the recovered costs.

Summary

The importance of online safety cannot be overstated. The Act has made many significant positive strides, however there are opportunities to expand its scope, strengthen enforcement tools, enhance governance structures, and explore sustainable funding models to keep pace with the rapidly evolving online landscape and safety challenges.

At Black Ink Legal, we recognise that the rapid advancement of technology, digital services and smart devices poses challenges and facilitates harms that impact everyone in modern society, and in particular, disproportionately impact the most vulnerable members of our society. Indeed, governments and communities around the world are contending with a digital ecosystem that is evolving at a pace that outstrips attempts to regulate and govern. With these rapid changes in technology and evolving community expectations, it is of vital importance that our regulatory and legislative frameworks must not remain static.

The Act has made significant advances towards promoting online safety through measures like establishing complaints schemes, setting expectations for service providers, and empowering the eSafety Commissioner. However, there remains (and likely will always remain) room for expansion and enhancement to better achieve the Act's objectives.

Overall, our response underscores the importance of the Act, together with its positive impact on online safety, whilst identifying opportunities to expand the Act's scope, strengthen enforcement mechanisms, enhance transparency, and adapt to evolving online threats through measures like statutory duties, international cooperation, and robust governance structures. Black Ink Legal commends the Department for seeking to constructively engage with stakeholders to inform the legislative reforms, and we welcome the opportunity to discuss any of the topics raised in this submission. We look forward with anticipation to the next round of consultation and updated draft legislation.

BLACK
INK
LEGAL