GNI Submission to the Australia Online Safety Act Review

Guiding Questions:

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?

During the drafting of the Online Safety Act in 2021, GNI raised concerns with the then Australian Minister for Communications about the categories of regulated services under the Online Safety Act being overly broad, which risked affecting certain types of services less proportionately than others. While GNI continues to be concerned about the scope of the regulated categories, recent developments within the online industry and advancements in global online safety governance indicate that eliminating these categories will be less suitable to the overall objective of the Act. GNI appreciates and supports the Australian Government's intention to keep pace with the evolving digital environment and maintain parallels with other global regulatory regimes. However, the existing categories that have undergone several rounds of review and are more specific to the Australian context would serve more effectively. The challenges that remain with scope of the categories can be addressed by tailoring them according to services' risk profiles and size.

To do this, GNI suggests replacing the blanket regulatory framework with a more systems-and-processes approach, i.e. introducing additional risk-based measures to differentiate services within the existing eight regulated sections that accounts, for example, for their levels of openness, use by children, size, reach, business models - including data collection practices - and governance models. The Government may consider necessary and proportionate human rights due diligence and impact assessment procedures to help determine the risk and severity of impacts on the users of services. The GNI Principles and Implementation Guidelines, as well as the broader, complementary approaches outlined in the UN Guiding Principles on Business and Human Rights ("UNGPs") and OECD Guidelines for Multinational Enterprises ("OECD Guidelines"), include robust guidance for how companies should conduct due diligence and assess risks associated with human rights. The Government should exercise transparency in this process in line with due process norms and these international business and human rights frameworks, and develop narrowly tailored risk evaluation criteria based on services' size, reach, risk, and impact.

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?

The Australia Online Safety Act includes many low-risk services in scope that are not currently accounted for within the eight regulated sections of online industry. In this regard, the Act is broader than some other regulatory approaches emerging in other regions, since it includes services that do not present concrete risks to or are not typically used by children. As such, the Act therefore creates unnecessary operating costs for low-risk services.

4. Should the Act have strengthened and enforceable Basic Online Safety Expectations?

The Basic Online Safety Expectations (BOSE) Determination came into effect in January 2022, and has not been in force for long enough to adequately identify its impacts. Any efforts to strengthen and/or enhance the enforcement of the BOSE must be based on an affirmative demonstration of the necessity and proportionality of such changes, and followed up with public and multistakeholder consultations prior to implementation.

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?

The code drafting process is overly fraught because of the broad scope of the Act itself and of the taxonomy used to classify services. For example, the "relevant electronic services" and "designated internet services" are imprecise groupings, and there have been difficulties associated with drafting obligations for services with diverse functionalities, use cases and levels of risk. More importantly, the ability of providers of in-scope services to address certain issues can vary depending on the functionality and privacy expectations of users (e.g.: expectations of privacy are higher on email than other services). It can also be difficult to identify the appropriate representatives for groups like the designated internet services.

6. To what extent should online safety be managed through a service providers' terms of use?

Under the Basic Online Safety Expectations of the Act, the Australian Government places the expectation on service providers to "ensure that the service has clear and readily identifiable mechanisms that enable end-users to report and make complaints about breaches of the service's terms of use." GNI believes that the current approach, which does not directly regulate services' terms of use, strikes a good balance by clarifying the government's expectations of covered service providers, while allowing them flexibility to apply approaches that adapt to different types of services and evolving circumstances. The Government should be careful to

ensure that any requirements it may consider imposing are justifiable under international human rights law, meaning that they consist of the least restrictive means of achieving a legitimate purpose and they are proportionate and appropriate to such purpose. The government should also take care to ensure that its approach respects the principle of comity and avoids unnecessarily impacting or creating potential conflicts of law regarding the rights of users not located in Australia.

7. Should regulatory obligations depend on a service providers' risk or reach?

Yes, risk and impact should be considered as the key metrics for determining regulatory approaches to harm. It is notable that no other jurisdiction has pushed for online safety legislation as broad as Australia. For example, Ireland's OSMR Act has a broad definition but the regulator is required to designate individual services by demonstrating risk, the UK's OSA also has very precise definitions of the most high risk services based on their reach, and the EU's Digital Services Act reserves its most significant obligations for Very Large Online Platforms and Search Engines.

In its Content Regulation and Human Rights Policy Brief, GNI recommends that the Government adopt "carefully considered approaches [and] narrowly tailored requirements that are targeted at services that pose the greatest risk of harm." Similarly, the UN Guiding Principles offer additional and more detailed guidelines on how risk and severity of a services' impact should be understood in terms of "their scale, scope and irremediable character." Reach is an important and relevant factor in and many similar laws around the world have adapted rules for smaller or new services to ensure their impact is not disproportionate.

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?

There are currently four complaints and content-based schemes under the Online Safety Act, and the eSafety Commissioner has the power to investigate complaints under these schemes and issue removal orders that mandate content takedown within 24 hours of notice. While GNI appreciates the tiered approach to addressing sexual abuse and cyberbullying against children

and adults - the threshold for regulatory action being higher in the case of the latter - to help ensure that freedom of speech is not unduly restricted, the application of 24 hour removal orders remain of concern.

As noted in the Content Regulation and Human Rights Policy Brief, the short window for takedown forces service providers to rapidly adjudicate the legality of third party content on their services, often resulting in over-removal. While service providers have important roles to play in addressing online harms, the Government should refrain from shifting all legal liability from those generating illegal content to intermediaries. The overly stringent enforcement and penalties under the OSA risk "unintended consequences and complicated implications for the rule of law, democratic process, accountability, and redress." GNI also reiterates that "the rigid 24-hour takedown provision creates the possibility that content that is newsworthy, time-sensitive or of a subjective nature may be censored without sufficient clarity or opportunities for appeal."

It also bears noting that, following the implementation of the Act, several laws have reproduced the stringent 24-hour takedown windows in other countries, including authoritarian jurisdictions where freedom of expression was already under threat.

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)?

Restrictions on children's access to content should be targeted and respond to public interest objectives. The Government should consult separately on these. Any proposals should continue to allow children to freely access essential digital services such as news media and email. Any provision and its enforcement needs to be mindful of the balance between protecting children but also allowing the exercise of their rights with evolving autonomy as it is laid out by the UN Convention on the Rights to the Child, and its General Comment No. 25 (2021).

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?

The framework set under the Basic Online Safety Expectations (BOSE) for service providers to take reasonable steps to minimize the presence of abhorrent violent content and support end-users with clear and readily identifiable mechanisms to report such content sets a good benchmark for measuring regulatory compliance. GNI appreciates the transparency that the Commissioner has maintained on the application of the BOSE since 2022.

In addition to the BOSE, the eSafety Commissioner has a broad mandate to block access to content that depicts, incites, promotes, or instructs abhorrent violent conduct under part 8 of the Act. The Commissioner alone is empowered to determine whether a material is likely to cause significant harm to the Australian community, and is able to issue blocking notices to a wide range of services. Furthermore, under division 1(3) of part 8, the Commissioner "is not required to observe any requirements of procedural fairness in relation to the giving of the blocking request," which is an exceptionally broad and unchecked power that could threaten freedom of expression.

While the OSA exempts certain material from blocking under Division 4 Subsection 104, including material that is necessary for investigation or enforcing the law of a country or material that relates to a news report that is in the public interest, there must be additional safeguards to prevent extraterritorial application and conflict of law with other countries. This is especially noteworthy in light of the latest Federal Court decision reversing an injunction to block the video of a Sydney church stabbing by X globally.

16. What more could be done to promote the safety of Australians online, including through research, educational resources and awareness raising?

Part 4 – Penalties, and investigation and information gathering powers

17. Does the Act need stronger investigation, information gathering and enforcement powers?

In Australia, in addition to powers to mandate transparency reporting through the Basic Online Safety Expectations, the eSafety Commissioner is able to investigate complaints or suspected breaches of the codes or standards under the OSA. This is supplemented with the power to obtain identity information or the contact details of an end-user of services where the Commissioner has "reasonable grounds to believe the information is relevant to the operation of the Act." These existing powers are already significant and broad in range, compared to equivalent regulators in other jurisdictions. The Government should consider introducing some additional due process safeguards to avoid negative impacts on free expression, including

enhanced transparency in the implementation of enforcement action notices, and refrain from expanding them further.

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?

The Act already, and quite broadly, addresses the enforceability of penalties against services based overseas under Article 23. In specific cases where the eSafety Commissioner faces practical challenges with reasonable enforcement, the disruption of services may be considered, but only as a last resort. Service disruption risks serious violation of international human rights standards that Australia meaningfully advocates for and upholds; they must be enforced as narrowly as possible and only within Australian territory.

Service restriction and the regulation of individual pieces of content are highly risky, and the Government should exercise extreme caution against any form of extraterritorial application, especially for larger and global platforms that are affected disproportionately under such laws. GNI instead encourages the Government to focus on approaches to ensure that service providers have the right systems and processes in place to meet their obligations.

20. Should the Commissioner have powers to impose sanctions such as business disruption sanctions?

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?

GNI recommends against adopting an overarching Duty of Care approach that would place overbroad obligations on platforms to proactively mitigate harms. In its place, the Australian Government may consider a systems and processes approach adopted by other rights-complaint laws. This includes focusing on risks stemming from the design, functioning, and use of services, as well as finding tailored approaches to assessing whether service providers have the measures in place to mitigate those systemic risks.

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?

Australia should seek to align any transparency requirements under the Act as much as possible with transparency measures in place under other rights-respecting online safety frameworks. It is also important for the Government to emphasize that relevant government agencies under the Act, including the eSafety Commissioner, need to exercise transparency with regards to the kinds of requests or demands that they are making of covered service providers.

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?

The Government may consider improving researcher access to data, however, this must be accompanied with great care so as to not violate users' right to privacy. In addition, it is important to ensure a way to synchronize any such measures with those being put in place under other rights-complaint laws.

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?

Prior to proposing an Ombuds scheme, the Government must first conduct an appropriate level of assessment to make the case for why such a scheme may be necessary and articulate how any proposed approach is consistent with international human rights law. At present, the Ombuds scheme described by the Government is exceedingly vague and lacks sufficient detail to generate meaningful analysis and response.

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

Yes, it is important that the Government guarantees access to remedy for both service providers and end-users of services. There should also be measures in place to prevent the abuse of reporting mechanisms, for example, penalties for users attempting to use complaints and grievance mechanisms to silence legitimate speech of other users. On the development of codes and standards, the Government and eSafety Commissioner should continue to ensure that different stakeholders are part of the process through collaboration and open consultations. The Government should take particular care around the application of the existing Act to email services, since users' expectations of privacy on these services are high and there are likely to

be tensions with the upcoming Privacy Bill. Many other jurisdictions have excluded email specifically because of the difficulties associated with balancing safety rules with the right to privacy. This has not hindered action against criminal content like CSAM, which takes place under separate and appropriately crafted laws or industry schemes.

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?

Australia's commitment to online safety should be consistent with the country's long-standing commitments to international human rights principles, including through its engagement in the Freedom Online Coalition,the Declaration for the Future of the Internet, and the Christchurch Call to Action. When framing proposed changes, it is important for the Government to consider how the Online Safety Act would affect new technologies, such as federated content hosting. GNI also echoes the concerns it highlighted in its previous submission on the industry standards in Australia, reiterating that the Act has the potential to "create barriers to the creation of new sites, platforms, and services, many of which have traditionally been developed through organic, academic, and/or non-commercial means," for which the Government must exercise great care with regulation.

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?

GNI strongly recommends the Online Safety Act to remain technology neutral, allowing different service providers to understand how a statutory duty of care or safety by design obligations apply to them based on their specific service and use.

Privacy enhancing technologies are at the core of the organic technical evolution of industry services in search of better serving their users. The safety by design approach should be mindful that protecting privacy and anonymity is a critical element for the exercise of the rights to freedom of expression and privacy. It is fundamentally important that in seeking to promote a safety by design approach, the ability to communicate privately is not undermined. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has detailed how encryption and other privacy-enhancing technologies provide the security necessary for the exercise of the right to freedom of opinion and expression in the

digital age. As highlighted by countless organisations and networks, including the Global Encryption Coalition, promoting approaches that would compel online platforms to undermine encryption infringes the privacy of users and undermines the security of the whole systems, leaving them vulnerable to exploitation by malicious actors.

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?