GNI Submission to Australian Government on Potential New ACMA Authorities to Combat Misinformation and Disinformation

I. Introduction

The Global Network Initiative (GNI) welcomes the opportunity to provide feedback on the exposure draft of the Communications Legislation Amendment (Combating Misinformation and Disinformation) Bill 2023 recently published for comment.

GNI is a multistakeholder collaboration that brings together 88 prominent academics, civil society organizations, information and communications technology (ICT) companies, and investors from around the world. Members' collaboration is rooted in a shared commitment to the advancement of the GNI Principles on Freedom of Expression and Privacy, which are grounded in international human rights law and the UN Guiding Principles on Business and Human Rights (UNGPs).

GNI welcomes and appreciates the Australian government's commitment to addressing concerns about digital content and conduct and acknowledges commitments to freedom of expression in the Bill and accompanying guidance note. In this submission, we detail some of the key concerns with the current approach — including the broad scope of companies and content in scope, privacy risks associated with information gathering powers, and the need for additional transparency and oversight of the Australian Communications and Media Authority (ACMA) in establishing new rules, registering codes, and putting forth new misinformation standards.

This insight is informed by GNI's years of experience working on rights-respecting approaches to addressing digital harms and engagement on related developments in Australia. In 2020, GNI conducted an analysis using human rights principles of existing and proposed governmental

efforts to address various forms of online harm related to user-generated content. After extensive consultations with GNI members and outside stakeholders, including governments, in a wide range of jurisdictions, GNI published a policy brief titled "Content Regulation and Human Rights: Analysis and Recommendations" ("Policy Brief"), which set out a range of observations and suggestions on how to regulate content in a manner that upholds and strengthens human rights. The Policy Brief informed our decision to share a Letter and Analysis on the Online Safety Act in May 2021, to sign on to the Joint Letter on Australia's Basic Online Safety Expectation (BOSE) in November 2021, and to share the October 2022 submission on the Industry Codes pursuant to the Online Safety Act.

II. Scope of Application

Both the scope of companies that might face obligations under the Bill and the definitions of mis and disinformation these companies would be required to address could be further refined and narrowed to mitigate freedom of expression and privacy risks.

We acknowledge the detailed definitions of digital platform services and corresponding "sections" of companies that might be covered by the Bill: content aggregation services, connective media services, and media sharing services. We also appreciate that the Bill excludes internet carriage services, SMS services, and MMS services from these definitions, and further clarifies that digital platform rules do not apply to email services or media sharing services without interactive features. However, the Bill could go much further in clarifying and tailoring potential requirements to specific services that takes into consideration how they function and the role they may play in relation to misinformation and disinformation. Among companies categorized within these broad "sections," compliance and implementation with rules, codes, and standards could have substantially different ramifications in practice. For example, it is unclear what measures to address mis and disinformation should be considered adequate for companies at different sizes and levels of maturity. Furthermore, Clause 30 in

Schedule 1 implies that obligations might apply uniformly across "sections" and need not be mutually exclusive, adding to concerns of a "one-size-fits-all" approach.

We acknowledge the commitment, detailed in the guidance note, that ACMA will not have the power to order removals of individual pieces of content under this Bill. However, both mis and disinformation are defined broadly, covering information that is "false, misleading, or deceptive," and "reasonably likely to cause or contribute to serious harm." Purveyors of disinformation must "intend[] that the content deceive another person," distinguishing it from misinformation. Additional criteria in the Bill detailing the concept of "serious harm" is broad and places a significant interpretation burden on companies. Furthermore, the wide range of exceptions under the excluded content for misinformation category, such as entertainment and satire, professional news content, educational content, and content authorized by government bodies, appear difficult to implement in practice. These provisions could contribute to companies taking a heavy-handed approach to enforcement and potentially restricting some legitimate, legal speech to avoid noncompliance, while also facing ambiguity in expectations for recording, reporting on, and otherwise addressing content in some of the excluded categories.

Here, it is critical to emphasize the many instances of abuse of "fake news" legislation worldwide, and the chilling effects that overly broad requirements can have on individuals regulating their own content and conduct online. As governments around the world look toward new models for content regulation, which are increasingly concerned with issues of mis and disinformation, the Government of Australia has an important role to play in setting a precedent for rights-respecting legislation.

GNI recommends:

- Clearly and precisely define what is prohibited, as well as who can be held responsible for failing to enforce the prohibition.

- Carefully consider which types of private services, at which layers in the ecosystem, are most appropriately positioned to address different aspects of misinformation and disinformation and tailor the approaches to those best positioned to address those concerns.
- Take into consideration the size and maturity of companies when considering companies processes and policies in place to address disinformation and misinformation.
- Ensure that content that is allowed in analog contexts is also permitted in digital form.

III. Privacy and Transparency

Through both the authority to set digital platform rules and the proposed information gathering powers, the Bill would provide substantial information gathering capabilities for the ACMA to scrutinize company practices and processes regarding mis and disinformation. GNI appreciates the need for improved transparency on the part of ICT companies about their efforts to address concerns about digital content and conduct, and GNI has advocated widely for laws and regulations rooted in transparency about company systems and policies. However, additional steps should be taken to further clarify protections for personal data, to ensure such information ACMA requests is secure, and to narrow the scope of information requested, including regarding information that can later be published by ACMA. The Bill should more clearly define the purposes and grounds on which information can be requested and the process that must be followed for requesting information.

The Bill provides authority for ACMA to designate rules requiring digital platforms to maintain records and report to ACMA on misinformation and disinformation on their service, measures to prevent or respond to such content (and their effectiveness), and the prevalence of content "containing false, misleading or deceptive information." Companies might face potential civil penalties for failure to comply. The ACMA also has the power to publish information received. We recognize that important exceptions have been included: requirements cannot be issued

for platforms to share private messages, ACMA must consider the privacy of end-users of the service when making a rule, personal information (within the meaning of the Privacy Act 1988) cannot be published, and ACMA must consult with companies prior to publication to allow them to identify information that might be "expected to prejudice materially the commercial interests of a person." However, more clarity should be given regarding the parameters that ACMA must follow when deciding to publish information and ACMA itself should be subject to more robust data protection obligations for how this information is collected, used, and stored.

GNI is also concerned by the scope of potential recipients of such information requests. The Bill enables authorities to request information from companies and persons who might not otherwise be covered by a code if the ACMA has an undefined "reason to believe" that they are relevant, in possession or capable of providing evidence on mis and disinformation on a service. The potential compliance burden and impact that these provisions may have on third parties such as fact-checkers should be considered.

GNI Recommends

- Put forth clearer guidance and expectations on the information companies should expect to report on and what information ACMA may seek to share publicly, without tying such requirements to disproportionate penalties.
- Tailor requests for information in ways that demonstrate respect for privacy and data protection and acknowledge and account for information shared through companies' transparency mechanisms.
- Recognize the value of strong encryption in protecting users, ICT services, and the ICT ecosystem and ensure it is clear that companies should not proactively monitor private content as part of their efforts to address disinformation and misinformation.

IV. Penalties and Enforcement

The Bill details a robust set of authorities for ACMA. In addition to the platform rules regarding recording and reporting of information noted above, ACMA would be able to call on industry bodies to put forth codes, which ACMA then reviews and registers. ACMA would have additional authorities to set standards, via legislative instrument, covering companies where industry bodies may not exist or otherwise fail to respond to requests, where ACMA identifies total or partial failures in implementing codes, or in undefined "exceptional and urgent circumstances," (a troubling precedent). Through setting digital platform rules, ACMA also has broad authority to designate additional companies as covered by the "sections" of industry cited above, and the Minister of Communications can also identify companies in scope via legislative instrument.

In each of these areas, the criteria and basis for regulatory authority could be more clearly spelled out to provide certainty for companies and reflect the careful consideration needed for regulator involvement in matters of speech. Clause 33 of Schedule 1 of the exposure draft, which details a set of potential examples of the types of matters that might be covered by misinformation codes and standards, lists a wide range of potential activities, but provides few parameters on the potential scope of codes or standards. In both reviewing codes for registration and in proposing potential standards to address alleged failures from companies, ACMA's standard for evaluation is ensuring that companies "provide adequate protection" from mis and disinformation, which is an overly broad approach. We also acknowledge some of the limitations put in place on the criteria for codes and standards, such as requirements to not cover private messages, and avoiding codes and standards that burden political communications. However, there could be much stronger and more explicit requirements for industry bodies and ACMA to identify and mitigate any potential privacy and freedom of expression risks associated with the development and registration of any codes or standards.

The Bill outlines several enforcement measures that are meant to be applied in a graduated manner, dependent on the harm caused, or risk of harm. This includes formal warnings,

infringement notices, remedial directions, injunctions, and civil penalties (up to 2% of global turnover for non-compliance with a code and 5% of global turnover for non-compliance with an industry standard). The range and significance of the enforcement measures are concerning given the complex nature and many gray areas of mis and disinformation and the challenge in identifying and addressing the same. Heavy-handed enforcement measures can result in over-compliance by companies and a loss of flexibility that may be needed to address misinformation and disinformation. In practice, they can shift the burden of identifying and removing misinformation and disinformation on digital platforms while not addressing the underlying societal causes of the issue.

GNI Recommends:

- Ensure that laws require transparency, oversight, and remedy.
- If authority is delegated to independent bodies, create robust oversight and accountability mechanisms to ensure that such bodies act pursuant to the public interest and consistent with international obligations.
- Refrain from overly stringent enforcement and penalties, to accommodate a diverse range of business models and capacities among covered businesses, as well as to foster innovative approaches to content moderation and guard against over-removal.
- Ensure robust remedial mechanisms for users whose content is restricted to avoid incentivizing self-censorship and over-removal.
- Build periodic reviews or reauthorizations into the law, to ensure that it remains relevant and consistent with evolving norms and technologies.

V. Conclusion

GNI acknowledges the Australian Government's efforts to strengthen cooperation on mis and disinformation in the online ecosystem, and we appreciate the focus on companies' systems and policies for addressing misinformation as opposed to individual content determinations. However, the broad definitions, breadth of services covered, and insufficient transparency and

oversight of the ACMA's proposed responsibilities in the Bill could entail serious risks for privacy and freedom of expression. The regulation of misinformation is an increasingly challenging discipline and requires substantial safeguards to privacy and expression, which could be better reflected in the Bill in its current form. In the presence of the voluntary code on disinformation and Basic Online Safety Expectations (BOSE) that may overlap with some of the newfound obligations, the current Bill could add to complexity digital services face in navigating through the legislative framework to address digital harms. The Bill could also risk complicating, or even undermining, progress made under existing voluntary measures by putting forth overly rigid approaches.

We therefore encourage the Government of Australia to consider these recommendations as they revise and update the Communications Legislation Amendments. GNI hopes that this feedback will be useful and remains eager to engage with Australian authorities, industry associations, and civil society to ensure that Australia's approach to online safety is consistent with the country's long-standing commitments to international human rights principles, including through its engagement in the Freedom Online Coalition and the Declaration for the Future of the Internet.