08 January 2024

Hon. Tiran Alles
Minister for Public Security of Sri Lanka
Floor 14, Suhurupaya, Subuthipura Road,
Battaramulla, Sri Lanka

Dear Minister Alles,

Asia Internet Coalition's Submission On The Draft Online Safety Bill, Sri Lanka

On behalf of the Asia Internet Coalition ("AIC") and its members, we are writing to express the concern and advocate for extensive revisions and overhaul of the Draft Online Safety Bill ("OSB") currently under consideration. While we appreciate the efforts made thus far with the industry, a more comprehensive and meaningful consultation is necessary to address the complexities and nuances associated with the Bill.

We acknowledge that the legislative process is intricate, and deliberations are ongoing. However, it is crucial to ensure that the Bill is not only effective but also balanced, proportionate, and practicable in its scope and approach. The proposed legislation, in its present form, poses significant challenges that, if not addressed comprehensively, could undermine the potential growth of Sri Lanka's digital economy. AIC's submissions, attached herewith, highlights various areas of concern from specific clauses ranging from regulatory independence and extraterritorial application to the overbroad definition of intermediaries, ambiguous terminology defining prohibited statements, divergence from international human rights and best practice standards, and more.

As part of the industry's continued engagement with the Government of Sri Lanka, please find attached to this letter key areas of concerns and recommendations. AIC is of the view that providing clause by clause edits would not adequately address the larger concerns we have identified in the draft bill. We firmly believe that, without extensive revisions, the proposed legislation will be unworkable.

Minister Alles,

The economic implications of the proposed Online Safety Bill cannot be overstated. Sri Lanka's digital ecosystem stands at the precipice of substantial growth, and it is essential to foster an environment that encourages innovation and investment. The concerns raised in our submission with regard to criminal liabilities, safe harbor provisions, turnaround times, user data access, and other critical aspects of the bill underscore the urgency of reconsidering the current draft.

We understand the complexity of drafting such legislation and acknowledge the importance of addressing online safety concerns. Therefore, this continued collaborative approach is essential to ensure that the Online Safety Bill strikes a balance between safeguarding users and fostering a conducive environment for digital innovation. We remain committed to working with the Government of Sri Lanka to create a more workable and effective Online Safety Bill that aligns with global best practices. In addition, the AIC has actively engaged with local stakeholders in Sri Lanka in the past to develop a comprehensive Sri Lanka Code of Practice for Online Safety and Responsible Content ("Code"). Drawing upon the expertise and insights gained through this collaborative effort, it is recommended that relevant elements from the code be considered and potentially integrated into the current bill. This collaborative and inclusive approach will further enhance the effectiveness of the Bill, ensuring a well-rounded and globally informed framework for addressing online safety concerns in Sri Lanka.

We kindly request the Government of Sri Lanka's thorough consideration of the issues highlighted in our latest submission. We look forward to engaging in further consultations and meaningful dialogues on the Online Safety Bill. Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490.

Thank you

Sincerely,
Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Key areas of concern and recommendations

We urge the Government to consider the concerns raised in this section.

1. **Broad and ambiguous definition of prohibited statements:** The Bill (Part III) outlines a wide range of offenses with overbroad and vague definitions. Such broad definitions are out of line with international human rights standards and fail the test of necessity and proportionality, as outlined in the International Covenant on Civil and Political Rights (ICCPR) which Sri Lanka has ratified. Such broad and ambiguous definitions are prone to misuse of the law by governments to suppress legitimate speech. Further, broad and ambiguous definitions create unpredictability and inconsistencies in the application of the law, both by courts and regulatory authorities, and prevent companies from being able to efficiently and effectively assess the legality of content. Clear, narrow, and precise definitions of prohibited content are necessary in order to enable platforms to adequately respond to legal removal requests, while reassuring these platforms and the public that the law has been carefully crafted to target illegal content while respecting fundamental rights to freedom of expression. In line with Sri Lanka's international human rights commitments, the Bill should recognize and ensure protection and respect of human rights, including Sri Lankan's fundamental right to free expression. Restrictions on the right to freedom of expression must be legitimate, proportionate and necessary and should take the following factors into consideration:

    - Prevalence: the number of people affected or likely to be affected by the content.
    - Severity: the degree of real-world harm caused or likely to be caused to the people affected.
    - Urgency: the immediacy of the harm or threatened harm.
    - Discrimination: whether takedown demands target particular population groups on the basis of race, religion, gender, sexual orientation or other protected categories.

2. **Duplication of existing laws**: The various offences in the Bill (Part III) that relate to 'prohibited statements', which incite others to commit offences, are already found in the Penal Code Ordinance, No. 2 of 1883, and therefore need to be either removed due to such new offences in the Bill being superfluous, or substantially revised in terms of their precision, and the rationality, reasonableness, and proportionality of the penalties imposed. The Bill should avoid duplication which can only lead to legal

uncertainty. Instead a review of existing legislation should be conducted to ensure consistency and regulatory certainty. Offences relating to religious feelings and terrorism in particular are already covered under specific legislation.

3. **Overbroad definition of intermediaries:** The Bill, in general, appears to reference a wide range of intermediaries, not taking into account the need to differentiate services according to levels of risks and functionalities. This creates a risk of over-regulation for a whole range of services, from simple websites and blogs to hosting providers, private messaging services, and social media. It is vital to take into account the fundamentally different roles played by different online service providers and platforms. It is also critical to avoid an overly broad and indiscriminate approach. Requirements placed on intermediaries should be relevant and fit for purpose. For example, what makes sense for content-sharing platforms may not be appropriate or technically feasible for a search engine, private messaging service or a platform that hosts mobile apps. The Bill should be limited in scope to relevant intermediaries, and should not apply to private communication services, such as one-to-one messaging platforms.

4. **Criminal liability:** The Bill (Part III) proposes fines and up to 5-20 years criminal liability for the communication of "prohibited statements", which may include an officer of an internet intermediary. The criminalization of illegal content, such as false statements, is a disproportionate restriction on freedom of expression. The bill criminalises all forms of prohibited statements regardless of whether they are likely to result in harm, and does not provide sufficient defence to individuals or intermediaries accused of the offence. Further, criminal penalties on intermediaries creates a hostile environment for business and would deter foreign direct investment. Therefore, criminal liability should be removed from the Bill.

    a. As noted in the U.S. International Trade Commission's report on foreign censorship, laws with criminal penalties, along with local representative requirements, are amongst the "censorship-enabling measures" that may enable or facilitate government suppression of speech. The report notes that, "While officially aimed at addressing concerns about harmful online content, these requirements, according to industry representatives, nongovernmental organisations (NGOs), and other stakeholders, instead make firms and their employees more vulnerable to government intimidation and harassment."

    b. Sri Lanka has been a signatory to the Universal Declaration of Human Rights since 1948 and ratified the International Covenant on Civil and Political Rights in 1980. Any proposed restriction, regulation, or criminalization of online speech must therefore reckon with these rights in order to pass international human rights scrutiny.

5. **Intermediary Liability:** The Bill (Clause 31) does not provide for reassurances as to the limitations of liability that platforms can benefit from if they do their best to act once notified of illegal content being present on their platforms. Liability for content must remain with the author/originator or publisher/uploader. Platforms should be treated differently than the author/originator

or primary publisher/uploader of the content served, linked, or hosted. Safe harbour should not be conditional upon compliance with all parts of the Bill or any rule made pursuant to the Bill. Internet intermediaries should not be considered responsible unless and until the intermediary has received notice of the illegal content. The Bill should recognise that when intermediaries follow their removal obligations under the law, such intermediaries should be certain that they will not be held liable for the hosted content. A clear "notice-and-takedown" regime should be expressly specified, that requires intermediaries to act expeditiously on illegal content upon notice from a court or independent regulatory authority. The Bill should provide clarity on the formalities for legal notices to be submitted to intermediaries, including:

- clearly identifying the content at issue by URL and where applicable, include, video timestamp, or some other unique identifier (not a second-level domain);
- clearly stating the basis of the legal claim, including the provisions of the applicable local laws and the country in which the law applies;
- clearly identifying the sender of notice, especially where the nature of the rights asserted requires identification of the rightsholder; and
- attesting to the good faith and validity of the claim using the legal form appropriate to the jurisdiction (such as an oath under penalty of perjury).

6. **Fixed turnaround times**: The Bill (Clause 26) requires intermediaries to comply within 24 hours from the issuance of a legal removal notice. Experience in other countries have shown that short turnaround times (e.g. 24 hours) for legal removal orders are not practical, do not have the intended safety effect, do not take into account the volumes of content being dealt with, and the need to conduct appropriate reviews of legal removal orders, especially with regards to the public interest and associated international human rights standards including the protection of freedom of expression and access to information. It is essential to note that content is not equal in harm. The severity of harm varies in which it is important to allow companies to conduct and prioritise requests according to the potential level of harm that content may cause. Response times to legal removal orders will vary case to case, depending on the complexities, volume of content under consideration, and completeness of information (e.g. URL, legal reasoning, etc). There are also legitimate variations between different technologies, different types of businesses, and different contexts. Companies need a reasonable period of time in which to assess the legal removal order once all the required information has been provided by the requesting authority. The 24-hour time frame for responding to a notice should be removed from the Bill and instead require online service providers to respond within a reasonable timeline on a best efforts basis, upon receipt of a clear, reasoned and complete notice.

7. **Due process rights and procedural safeguards**: The Bill does not set out a process through which affected parties can be heard by a court of law during the Online Safety Commission's investigation, or a process for appeal to an independent body against legal removal notices. This is inconsistent with Article 12(1) of the Sri Lankan Constitution, which the Supreme Court of Sri Lanka has interpreted to include the right to be heard. The Bill should provide individuals and companies an opportunity to be heard or appeal when a legal removal notice is issued.

8. **User data and system access**: The Bill (Clause 28 and 29) gives the proposed Online Safety Commission (OSC) powers to issue legal removal orders to intermediaries to disclose the identity of the uploader, if unknown. The police may also seek access to subscriber information, computer systems, traffic data, communications, etc. as part of their investigations of these offences. Besides being very broad and potentially very cumbersome, this requirement includes information that is likely to be highly sensitive, for example details around users, service pricing and key service developments, some of which could be considered trade secrets. Requests for user data made to foreign-based service providers outside the proper, legitimate international channels may create conflicts with foreign law. Further, internet intermediaries may be required to break end-to-end encryption in order to disclose identification information, which is technically impossible without fundamentally altering the architecture of encrypted platforms. The Bill should follow established procedures of international law, including treaty-based and other diplomatic procedures, to seek disclosure of user data held by companies.

9. **Extraterritorial application:** The Bill (Part III and Clause 34) appears to have extraterritorial application as it applies to "any person, whether in or outside Sri Lanka". Different countries may have conflicting laws and legal systems. Applying one country's laws extraterritorially can lead to conflicts and confusion about which laws should take precedence. Imposing extra-territorial application is not a global practice, thus may put Sri Lankan businesses at a disadvantage since this is applied unilaterally by the government, and may prompt reciprocal measures from other governments.

10. **Independence and powers of the Online Safety Commission:** The Bill (Part II) provides the newly established Online Safety Commission (and the Minister) expansive powers, while granting the President unprecedented and unfettered discretion in appointments of members to the OSC, which raises concerns about accountability and potential misuse. The exercise of powers and functions by an institution lacking independence from political interference threatens the freedom of speech and expression. Regulators should enjoy structural independence to reduce the possibility of political interference and to ensure that it is accountable to a broad spectrum of stakeholders. People should have confidence that OSC decisions are objective and transparent. The OSC should have a formal requirement to consult with a wide variety of stakeholders (including companies, NGOs, academics) and to give due regard to their input in developing rules *vis a vis* codes of practice for online safety. This will encourage regulators to build rules that reflect the broad interests of society as a whole rather than those of particular individuals

or entities. Further to this, the powers of the regulator should be subject to principles of proportionality, constitutionality and due process. Appointment of members to the OSC should be conducted through an appointment mechanism that guarantees its political independence. The Commission should not be vested with quasi-judicial powers, nor with powers to designate online locations as 'declared online locations. The Bill should be amended to reflect all of this.

11. **Registration with Online Safety Commission**: The Bill (Clause 11 and 53) empowers the OSC to specify the manner in which online service providers shall be registered. Registration or licensing is usually required where resources are scarce and operators obtain something of value in return for a licence, such as spectrum for mobile, TV or radio channels. When it comes to online services, there are a number of services that can be offered which do not require the allocation of such finite resources. While many governments see these policies as simple solutions to the challenges of a complex global economy, the truth is that the drawbacks for a country and its companies far outweigh the benefits. Instead, local registration efforts reduce that country's competitiveness across all local economic sectors and undermine the health of the global economy by raising the cost of doing business internationally. A study conducted by European Centre for International Political Economy on forced localization found that the negative economic impact of such policies on GDP for these seven countries/regions were as follows: Brazil -0.2%; China -1.1%; EU -0.4%; India -0.1%; Indonesia -0.5%; Korea -0.4%; Vietnam -1.7%. For these reasons, requirements for registration should be removed from the Bill.

12. **Codes of practice**: The Bill (Clauses 11, 30 and 53) broadly empowers the OSC to introduce rules *vis a vis* codes of practice, without providing procedural guidance or safeguards on the conditions, criteria and process that would warrant such rules being introduced. As noted above, the OSC should have a formal requirement to consult with a wide variety of stakeholders (including companies, NGOs, academics) and to give due regard to their input in developing rules vis a vis codes of practice that would be relevant, practicable/implementable, and fit for purpose. An example of such a code is the civil society led "Sri Lanka Code of Practice for Online Safety and Responsible Content" ("Code"), which went through a comprehensive and extensive consultation with key stakeholders — including industry, NGOs and government — to ensure legitimacy, support, workability and future compliance with the Code. The Bill should consider the incorporation of the Code, while narrowing the scope and focusing the Bill on establishing a notice and takedown legal regime that adheres to international human rights standards and regulatory best practices.

13. **Legislative consultation**: Ongoing dialogue between Government and stakeholders is an important part of policymaking. This is to ensure lawmakers have a comprehensive and diverse understanding of how a policy may impact the various stakeholders, either directly or indirectly. Conducting a thorough and comprehensive consultation throughout the policy development process helps facilitate and foster that understanding. The Bill was introduced without any prior stakeholder consultations, resulting in

an unworkable draft that has raised a wide range of concerns by tech companies, civil society, other governments, and the international community. These stakeholders, at minimum, should be engaged in a meaningful and comprehensive consultation process to inform future amendments and iterations of the Bill, before it is passed.