

**Asia Internet Coalition (AIC) Industry Submission On The Draft Online Safety Bill,
Sri Lanka**

1 December 2023

To
Hon. Tiran Alles
Minister for Public Security of Sri Lanka
Floor 14, Suhurupaya, Subuthipura road,
Battaramulla, Colombo 00700, Sri Lanka

Dear Minister Alles,

On behalf of the Asia Internet Coalition (“AIC”) and its members, I am writing to share our appreciation at the opportunity to submit the comments below on the proposed Online Safety Bill. AIC is an industry association of leading internet and technology companies in the Asia Pacific region with an objective to promote the understanding and resolution of Internet and information and communication technology policy issues. AIC and its members are fully committed to the cause of a safe and open internet.

The proposed Online Safety Bill risks having a significant adverse impact on the economy of Sri Lanka. The Bill would impose a significant and concerning compliance burden, threatening to deter investment in Sri Lanka’s digital ecosystem by imposing harsh criminal liabilities, limited safe harbour protections, unreasonable and unworkable turnaround times, and broad user data access requirements – all of which are granted to a regulator that lacks independence or offers clear appeal mechanisms. Its overbroad and vague definitions of terms such as “facts,” “false statements,” and “feelings of ill-will” also raise the concern for significant abuse, misunderstanding and threats to users’ ability to access and use information and knowledge. Together, these features of the Bill risk harming the growth of Sri Lanka’s digital economy, which has enormous potential given Sri Lanka’s young and increasingly digitally savvy population.

The economic benefits of Internet platforms extend to virtually every corner of the economy, driving growth in sectors from tourism to textiles. Internet platforms stimulate employment and entrepreneurship, most notably for SMEs. The online creator economy is a major engine for economic opportunity and creative growth, creating thousands of jobs and connecting people all over the world with entertainment, information, and inspiration. Internet platforms have brought unprecedented consumer empowerment. They boost innovation and productivity. And they contribute to efficient markets and trade by bringing suppliers and consumers closer together. Internet platforms are major catalysts for information and knowledge diffusion: search engines, portals, and participative networked platforms facilitate access to an unparalleled wealth of information, and to opportunities for new activities and social interactions, learning, culture, and work. Vast numbers of people are able to create and introduce many kinds of content, on a broad and often global scale, with wide-ranging impact on the way users produce, distribute, access and re-use information, knowledge and entertainment. In economies which increasingly rely on knowledge, this is having an important positive impact - for instance through Sri Lankan creators using online platforms to reach a global audience.

We support the Government of Sri Lanka's aim of creating legislation in line with constitutional principles of freedom of expression and global best practices and standards, which the international community and industry has long called for. It is important to note that well designed regulation and frameworks can foster a productive digital environment in Sri Lanka that upholds fundamental rights, encourages innovation, and ensures online safety, all of which together will facilitate a thriving ecosystem for new business investments. Legislation that is overly broad, ambiguous, and unclear risks government overreach and misuse and potentially leads to unintended and adverse consequences that might make people less safe online, stifle free expression, slow innovation, and impact future business opportunities and investments in Sri Lanka.

We recommend that content regulation focus on three key aspects: regulatory obligations, a clear and balanced liability framework, and defined, appropriate enforcement mechanisms, in line with international best practices. Regulatory obligations should include (1) clear definitions of prohibited content, (2) obligations tailored to the specific types of service, and (3) meaningful transparency reporting on outcomes that are tailored to the institutional arrangements of Sri Lanka. As currently drafted, the Bill's safe harbour conditions are too broad. Effective safe harbours should not be conditional upon rules issued by a regulator. Limitations on the liability of platforms for the actions of users have encouraged the growth of the Internet and its ensuing socio-economic benefits. 'Safe harbour' laws treat platforms differently than the author/originator or uploader of the content served, linked, or hosted. This helps to create shared responsibilities, ensuring that illegal content is addressed expeditiously while preserving economic growth, the free flow of information, and other societal benefits.

This framework should also include graduated, proportionate penalties for *systemic* failure (not one-off mistakes); that includes having no criminal, personal liability as that would lead to the risk of over-removal for fear of being subject to these onerous sanctions. And a Good Samaritan clause can incentivise responsibility.

The draft Online Safety Bill has several areas that are of significant concern to industry, discussed in detail below. We kindly request that the Government of Sri Lanka consider the issues highlighted in this submission and provide the AIC with an opportunity for further engagement and consultation on this consequential piece of proposed law.

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)

SPECIFIC AREAS OF CONCERN AND KEY RECOMMENDATIONS

1. Lack of regulatory independence in the proposed Online Safety Commission

- **Concern:** The newly established Online Safety Commission (and the Minister) would have expansive powers and the Bill grants the President unprecedented and unfettered discretion in appointments.
- **Recommendation:** Regulatory independence builds trust. As currently drafted, the Bill grants the President unprecedented discretion in appointments, raising concerns about accountability and potential abuse. Governments should empower regulators with a distinct legal mandate that is free of Ministerial control. 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. All stakeholders should have confidence that regulatory decisions are objective and transparent. Regulators 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 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.
- An effective regulatory framework to address harmful content, including government notice and takedown requests (TDR), must be guided by four key principles:
 - **Shared Responsibility:** tackling illegal content is a societal challenge—in which companies, governments, civil society, and users all have a role to play.
 - **Proportionality:** Defining the parameters of “control” – and the corresponding parameters of what constitutes reasonable and proportionate remedial action.
 - **Fairness and transparency:** Support companies’ ability to publish transparency reports about content removals, and provide people with notice and an ability to appeal removal of content.
 - **Rule of law and creating legal clarity:** It’s important to clearly define what [ISPs / Internet intermediaries / social media companies] can do to fulfill their legal responsibilities, including removal obligations. An [ISPs / Internet intermediaries / social media companies] that takes other voluntary steps by use of automated technology to address illegal content should not be penalized and should not lose its safe harbour protection. This is crucial, as it allows companies to go above and beyond the requirements where appropriate, including such voluntary efforts.

2. Extraterritorial Application

- **Concern:** Clarity is also needed on whether the Bill intended to have extraterritorial application, given that it applies to “any person, whether in or outside Sri Lanka”.

- **Recommendation:**

- We would also like to seek clarification that the provision will have no extraterritorial application.
- 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.

3. Overbroad definition of intermediaries

- **Concern:** This bill would regulate a whole 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 and social media.
- **Recommendation:** 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. For example, what makes sense for content-sharing platforms may not be appropriate or technically feasible for a search engine or for a platform that hosts mobile apps.

4. Vague and broad terminology defining prohibited statements

- **Concern:**
 - The Bill outlines a broad range of offenses with overbroad or vague definitions, including on the 'communication of false statements.' (e.g. 'Any person, whether in or outside Sri Lanka, who poses a threat to national security, public health or public order or promotes feelings of ill-will and hostility between different classes of people, by communicating a false statement, commits an offense..') and content deemed harmful, with subsets of offenses pertaining to religion, contempt of court, rioting, cheating, doxxing-type harassment, or false statements with '.. intent to cause any officer, sailor, soldier, or airman in the navy, army or air force of Sri Lanka to mutiny, or with intent to cause fear or alarm to the public...'. This extends to prohibiting the display of paid content including advertising for a website deemed to host such content by the online safety commission.
 - Vague and broad 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. Clarity in definition would allow companies to be more efficient and expeditious in responding to take down requests.

- **Recommendation:** Clear and precise definitions of online safety concerns are necessary in order to enable platforms to adequately respond to Government legal removal requests, while reassuring these platforms and the public that the law has been carefully crafted to target only content defined as illegal, thereby preserving freedom of expression and the free flow of information, in line with international human rights commitments. Restrictions on the right to freedom of expression must be legitimate, proportionate and necessary. In assessing whether the removal or blocking of content is proportionate, we recommend the following factors - in adherence to international human rights - be taken into consideration: prevalence, severity, urgency, and discrimination.
 - 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.

5. Registration requirement with the proposed Online Safety Commission

- **Concern:** The Bill requires Internet platforms to register with the Online Safety Commission, which will be established pursuant to this new legislation. The details of such registration remain unclear at this stage. Registration requirements, akin to licensing or pre-authorisation schemes, represent an administrative burden and can discourage certain providers from providing their services in the country, and can also stifle free expression by requiring permission from the Government to operate. Additionally, they would be difficult to enforce on providers based outside the country, thus either proving discriminatory for providers operating locally, and/or potentially preventing local citizens from accessing cross-border services.

Additionally, we believe that there is a fundamental difference between services that are delivered over the Internet and more traditional services like telecom and broadcasting. Licensing is usually required where resources are scarce and operators obtain something of value in return for a license, such as spectrum for mobile, TV or radio channels. When it comes to online services, there is a virtually infinite number of services that can be offered which do not require the allocation of such finite resources. As such, we do not believe that a licensing regime is appropriate for online applications and services. Looking at services referred to as ‘Video OTT platforms’, such Internet applications and services have been essential for economic growth and other societal benefits, including choice, innovation and new uses for consumers and businesses. It is important to note that these services are different from traditional, legacy broadcasting services, and therefore it would be impractical and beyond the capacity of any regulator to license all online services.

Moreover, local registration requirements will have negative and unintended consequences as explicated below:

- **Limiting consumer access to technology:** The economies of scale achieved through globally located infrastructure have contributed to the affordability of services on the Internet, many of them available for free. Companies are able to provide these services to users even in markets that may not be financially sustainable as they don't have to incur the additional cost of setting up and running local offices and legal entities in each country where they offer services, thereby enabling certain countries to benefit from products, services and information that they would otherwise have been unable to enjoy, thus considerably limiting their socio-economic development. Therefore, changing this virtuous dynamic by requiring local registration will harm economic potential as well as consumer experience on the open Internet whilst increasing costs.
- **Reduce competitiveness of a nation:** 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 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%.
- **Restrict Growth of SMEs and Stifle Innovation:** Local presence requirements artificially restrict SMEs' market and growth prospects by limiting their ability to engage potential partners and resources. SMEs rarely have the resources to invest in local offices in every market to which they seek to expand digitally. These requirements thus deny economies the opportunity to benefit from cutting-edge services, limit the innovative potential of economies, and deprive local companies and consumers of a wider array of less expensive choices.
- **Recommendation:** We therefore recommend removing the requirements for pre-registration of services, as will stifle innovation, creates onerous requirements for businesses and raises questions concerning enforcement and free flow of information.

6. Conditional safe harbour

- **Concern:** The safe harbour described in the Bill is very restrictive, thus not providing 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.

- **Recommendation:** Internet platforms have long had content policies that set the boundaries of what content is and is not permitted. This responsible approach to the operation of Internet platforms depends on and must be underpinned by thoughtful and fair legal frameworks when it comes to liability for illegal content, based on 'safe harbour' principles.

Limitations on the liability of platforms for the actions of users have encouraged the growth of the Internet and its ensuing socio-economic benefits. 'Safe harbour' laws treat platforms differently than the author/originator or primary publisher/uploader of the content served, linked, or hosted. This helped to create shared responsibilities, ensuring that illegal content is addressed expeditiously while preserving economic growth, the free flow of information, and other societal benefits. 'Safe harbour' laws usually incorporate a 'notice-and-action' approach which requires intermediaries to review, and where appropriate remove, specific illegal content expeditiously when notified.

We would strongly recommend that Sri Lanka's policymakers consider a "safe harbour" framework for Internet platforms based on well established international best practice, in order to provide the necessary clarity and flexibility, allowing businesses to operate and grow, and for Internet platforms to act on illegal content, without unduly compromising fundamental rights. In considering how to tackle inappropriate, harmful and illegal content online, Internet intermediaries are usually not in the same position as the originator of content to delete or edit the originator's content. Similarly, an intermediary is not in the same position as an originator to defend their post, such as a potentially defamatory statement.

Indeed, what many platforms do provide is a service / noticeboard for users to post user-generated content. Therefore, any proposal to subject such platforms to liability is unnecessary and excessive, noting that these platforms are just making a service available to users for posting and should not be penalized for their users' actions over which the platforms have no control.

For these reasons, liability for content must remain with the actual originators. To reflect the practicalities of dissemination of inappropriate content through Internet infrastructure, Internet intermediaries should not be considered responsible unless and until the intermediary has received notice of the illegal content, or unless the intermediary itself created the content concerned. Whether an intermediary is considered to have been put on notice of an originator's publication should depend on the intermediary's specific awareness of the potentially illegal nature of the material. The circumstances in which such awareness, and thus liability, should be attributed to an intermediary (rather than resting solely with the originator) should be dealt with clearly in legislation.

- **Specific suggestion:**
 - Safe harbour principle - the legislation 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: platforms should indeed 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 indeed any rule made pursuant to the Bill.

- Instead, a clear "Notice-and-takedown" model should be expressly specified, that requires intermediaries to act expeditiously on illegal content upon notice from a court. The notice system should provide clarity on the formalities for users to submit notices 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).
- Service Providers should be given flexibility in determining how to implement these requirements in practice.

7. Turnaround times and the absence of appeals procedures

- **Concern:** - Similar proposals for content regulation laws in other countries have proved that short turnaround times (i.e. 24 hours) at the risk of losing its safe harbour, are not practical and 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 norms 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 prioritize TDRs according to the potential level of harm that content may cause. Another related notable issue is that there is no provision for the affected person to appeal against the notice issued by the Commission, which is a significant shortcoming and no indication of how checks and balances will be ensured on the powers of the Commission. The above suggests that the Bill lacks proper procedural safeguards and due process.
- **Recommendation:** The exact time frame for responding to a notice is not something that should be stipulated in legislation, as it will vary from case to case, depending on the complexities and volume of content under consideration. There are also legitimate variations between different technologies, different types of businesses, and different contexts. Internet Service Providers also need a reasonable period of time in which to assess the take down request once all the required information has been provided by the requesting individual. For example, we regularly receive overly broad removal requests, including from public authorities, and analyses of cease-and-desist and

takedown letters across several jurisdictions and have found that many seek to remove potentially legitimate or protected speech. Specifically, we recommend the following legislative wording: “Timeline for response: Requests should be responded to as soon as reasonably practicable, upon receipt of a clear and specific notice.” We also recommend that the Bill include a clear and precise appeal process to an independent body.

8. User data and system access

- **Concern:** Under the Bill, the proposed Commission can seek an order for the intermediary 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 offenses. 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.
- **Recommendations:**
 - User data access: Regulations should follow established procedures of international law, including treaty-based and other diplomatic procedures, to seek disclosure of user data held by the global social media companies. Requests for user data made to foreign-based service providers outside the proper, legitimate international channels may create conflicts with foreign law.
 - General access to data: such requests for company, market or user information will be highly sensitive and are likely to trigger authorizations at the highest levels of the respective organization. The issue is made worse by the fact that:
 - these rights are broad and are not restricted to the activities conducted in the country nor data related to the delivery of services in the country;
 - international digital content service providers will be subject to both contractual obligations and the requirements of foreign law that may be breached if certain of this information is disclosed; and
 - the infrastructure used to provide digital content services is usually centralized. Disclosing sensitive information about the structure and nature of these arrangements could give rise to information security risks, which must be minimized in the provision of any secure, cloud-based service for the public.
 - We therefore recommend that the scope of these powers is restricted to activities conducted in the country and all requests are tied to ensuring that the company in question is complying with the requirements of local law or to investigating a reported breach of the law, as is customary under international law.

9. Criminal liability

- **Concern:** The Bill proposed fines and up to 5-20 years criminal liability. Failure to comply with any directive of the Commission to stop the communication of any prohibited statements within 24 hours of receipt is punishable with imprisonment of up to 5 years (and possibly up to 20 years) or a fine of 1 million rupees. This could apply to an officer of an internet intermediary which fails to comply with an order issued pursuant to the Act. Further, the intermediary could be held liable to pay compensation to the affected person for any wrongful loss caused by the illegal communication. An appeal in front of the Magistrate court is possible within a week of the order / notice being issued. The proposed punishments and sanctions in the draft bill are disproportionately hefty, including fines and imprisonment ranging from one to twenty years. The absence of judicial review and protection for the Commission and experts from legal scrutiny further raises considerable concerns about accountability and potential misuse of power.
- The U.S. International Trade Commission's [report](#) on foreign censorship notes that 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 organizations (NGOs), and other stakeholders, instead make firms and their employees more vulnerable to government intimidation and harassment.”
- **Recommendations:** Fines and imprisonment should be a last resort in the regulatory toolkit. Fines should be limited to systematic failures rather than for individual content violations. We would also recommend the removal of imprisonment from the sanctions. Effective enforcement should focus on systemic, intentional failures. We recognize the need for appropriate sanctions for a platform's systemic failure to comply with its duties. In such cases, companies / services in scope need a clear understanding of what constitutes a 'systemic failure' so they have a reasonable path to compliance. These include:
 - Defining systemic failures: An assessment of systemic failure should take into account: (1) the overall scale at which Service Providers operate; (2) Service Providers overall success rate at addressing problematic content; (3) the risks to [the respect of international norms including human rights / legitimate speech] from precipitous action; and (4) the need to take the time to orient to and understand novel issues as they arise.
 - Identifying systemic failures: An oversight body's primary means of identifying systemic failures should be the transparency reports produced by Internet Service Providers. This will enable the oversight body to investigate a platform's suspected failure to effectively implement its content guidelines.
 - Information and enforcement notices: Where systemic failures are identified, information and/or enforcement notices should privately be given to a service provider, affording it a reasonable opportunity to investigate and - if necessary - take appropriate action.

- Sanctions for non-compliance: If identified issues continue unrectified, then an oversight body should be permitted to issue proportionate sanctions for systemic failures. These sanctions should take into account the scale of the systemic failure, and be careful to avoid perverse incentives for companies to block legitimate content to avoid harsh penalties, and also afford the suspected company the opportunity to provide clarifications or appeal the decision. Sanctions may include the ability to issue information and enforcement notices, and as a last resort, to impose administrative sanctions and/or fines where necessary.

We recommend removing criminal liability directly from the Bill given that it creates a hostile environment for business.

10. Duplication of existing laws

- **Concern:** Some of the offences in the Bill appear to be at least partially covered in existing laws. For example with regard to offences which offend religious feelings, there are laws which cover similar ground, and the implementation of these laws has already been highly problematic. Section 2(1)(h) of the Prevention of Terrorism Act already makes it an offence for any person to cause or intend to cause the ‘commission of acts of violence or religious, racial or communal disharmony or feelings of ill-will or hostility between different communities or racial or religious groups’, by words, signs, visible representations or otherwise.’

Additionally, Section 291A of the Penal Code provides that uttering words deliberately intended to wound religious feelings is an offence punishable with imprisonment for a term up to one year, or a fine, or both.

Section 3 of the International Covenant on Civil & Political Rights (ICCPR) Act criminalises the propagation of war or the advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (however the threshold for offences here is higher than simply the ‘intention of hurting religious emotions,’ there must also an incitement to discrimination, hostility and violence’). The misapplication of this section in recent years has already attracted criticism.

- **Recommendation:** The law 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.