

## GNI Recommendations on Amendments to Sri Lanka's Online Safety Act

The [Global Network Initiative](#) (GNI) is the leading multistakeholder forum for accountability, shared learning, and collective advocacy on government and company policies and practices related to technology and human rights. GNI is a [membership](#) organization comprising over 100 academics, civil society organizations, investors, and technology companies. We have members on every populated continent, with nearly one-third based in the majority world.

GNI [reiterates](#) its appreciation for the Government of Sri Lanka's efforts to revisit and revise the amended *Online Safety Act (OSA) 2024*. We commend the commitment to engage in a more participatory and transparent legislative process and recognize this as an important step toward ensuring that digital policy reforms are grounded in respect for human rights and the rule of law. GNI has been closely following the development and implementation of the OSA since it was initially proposed, and we [remain](#) deeply concerned about several provisions in the law that pose significant risks to freedom of expression and privacy. These concerns include the broad and vaguely defined categories of prohibited content, the establishment of an Online Safety Commission lacking adequate independence or regulatory oversight, disproportionate penalties for online speech, and the absence of robust safeguards for user rights and data protection. These elements of the law, if left unaddressed, threaten to undermine the rights of Sri Lankans to freely and safely express themselves, access information, and engage in democratic debate online. They may also have chilling effects on civil society, media freedom, and innovation in Sri Lanka's digital economy.

GNI encourages the Government of Sri Lanka to ensure that any review process is open, transparent, and meaningfully inclusive of all stakeholders - including civil society, the private sector, technical experts, academia, and affected communities. Such an approach is essential to fulfilling Sri Lanka's obligations under its Constitution and its commitments under international human rights law, including the International Covenant on Civil and Political Rights (ICCPR). In support of these ongoing reform efforts, GNI offers the following analysis of specific provisions in the OSA that are inconsistent with international human rights law, along with corresponding recommendations rooted in our policy framework on content regulation and human rights.

GNI's [Content Regulation and Human Rights Policy Brief](#) (CRPB) analyzes more than 20 governmental initiatives globally that claim to address various forms of online harms and offers practical guidance for governments and other stakeholders on how to formulate and implement content regulations that are effective, fit-for-purpose, and enhance and protect the rights to

freedom of expression and privacy. The report is the result of months of multistakeholder analysis by GNI’s diverse, expert membership, and draws on internationally recognized principles of legality, legitimacy, necessity, and proportionality for the development of a transparent, accountable, and rights-respecting framework of digital governance. The table below outlines GNI concerns with the OSA and proposes relevant reforms, with the aim of assisting policymakers, civil society, and other stakeholders in building a revised legal framework that protects users’ rights while promoting online safety.

Problematic Provisions in OSA	GNI recommendations
<p>Section 12 – Penalizing vague “false statements”</p> <p>The provision uses vague and overly broad terms like “false statements” and “public disorder,” which can be misused to suppress dissent and protected expression.</p>	<p>Clarity, Legality, and Proportionality of Definitions:</p> <ul style="list-style-type: none"> <li>• All restrictions on speech must meet the three-part test: legality, legitimacy, and necessity/proportionality.</li> <li>• Vague terms like “false statements” or “causing public disorder” must be replaced with narrowly defined offenses, tied to actual, imminent harm. The Act should require demonstrable, imminent physical harm rather than abstract concepts like “feelings of ill-will” and “hostility between different classes of people.”</li> <li>• </li> <li>• Limit the Act’s jurisdiction to content created and hosted within Sri Lanka’s territorial boundaries.</li> <li>• Introduce a statute of limitations to prevent retroactive application to historical online content.</li> <li>• Explicitly excluding satire, artistic expression, and legitimate political discourse from the definition of prohibited content.</li> </ul>
<p>Sections 14–17 – Criminalizing religious insult/offensive content</p>	<p>Repeal for the Protection of Freedom of Expression:</p>

<p>These sections risk criminalizing speech based on subjective offense, potentially targeting critics, minorities, or journalists, and infringing on freedom of religion and expression, and therefore must be repealed.</p>	<ul style="list-style-type: none"> <li>● Criminalizing “hurt feelings” or “religious insult” is incompatible with international human rights law, unless they directly incite violence or discrimination.</li> <li>● Avoid creating criminal laws that can be weaponized against critics, minorities, or journalists.</li> <li>● Establish a clear test for criminalization of very narrowly defined content (e.g. incitement to genocide) that requires establishing intent to incite violence or discrimination, requires context to be taken into account, and emphasizes the importance of demonstrating impact and imminence.</li> </ul>
<p>Section 5 – Online Safety Commission appointed by President</p> <p>Centralized appointment without effective checks risks politicization and lack of accountability in online content regulation.</p>	<p>Independent Regulatory Oversight:</p> <ul style="list-style-type: none"> <li>● Establish an independent and impartial Commission, with appointments made through a transparent, participatory process involving civil society and parliamentary approval.</li> <li>● The Commission’s powers should be clearly defined, limited, and subject to judicial review.</li> <li>● Ensure the body is structurally separate from executive control to avoid political misuse.</li> </ul>
<p>Harsh penalties</p> <p>Imposing excessive penalties for speech-related offenses or noncompliance may chill free expression and disproportionately impact vulnerable voices.</p>	<p>Due Process and Proportionality:</p> <ul style="list-style-type: none"> <li>● Sanctions must be proportionate and follow fair procedures.</li> <li>● Avoid excessive fines or imprisonment for non-compliance with regulatory orders, particularly if they affect journalistic or public interest speech.</li> </ul>
<p>Section 35 – Search and seizure powers</p>	<p>Privacy and Data Protection:</p> <ul style="list-style-type: none"> <li>● All investigatory powers (e.g., device</li> </ul>

Broad investigatory powers without strong safeguards pose serious threats to user privacy and could lead to abuse.	<p>searches, data access) must require advanced judicial authorization and adhere to necessity and proportionality principles.</p> <ul style="list-style-type: none"> <li>● Introduce strong data protection safeguards, including notice, right to object, and independent oversight.</li> </ul>
<p>Section 45 – Immunity from legal action</p> <p>Blanket legal immunity for officials undermines accountability and weakens public trust in enforcement mechanisms.</p>	<p>Accountability and Redress:</p> <ul style="list-style-type: none"> <li>● Ensure meaningful access to remedy and redress for users.</li> </ul>

Necessary Additions to the OSA	GNI Recommendations
Data Protection	<p>The OSA is incompatible with Sri Lanka's Personal Data Protection Act (PDPA), as such, it should include:</p> <ul style="list-style-type: none"> <li>● Language requiring the OSA to comply with PDPA standards.</li> <li>● Explicit data minimisation requirements limiting collection to what is strictly necessary.</li> <li>● Ensure protection for encrypted communications and prohibition on compelling platforms to break encryption.</li> </ul>
Protection of Minorities and Preservation of Historical Memory	<ul style="list-style-type: none"> <li>● Make explicit exemptions for archives, museums, and educational institutions.</li> <li>● Ensure protection for documentation of human rights violations and historical events.</li> <li>● Include special safeguards preventing disproportionate targeting of vulnerable and minority communities.</li> <li>● Recognize memorialization as a protected form of expression.</li> </ul>

Remediation and Public Interest Litigation	<ul style="list-style-type: none"> <li>● Include provisions to allow for remediation of wrongful content removal or prosecution.</li> <li>● Ensure public reporting of all OSA enforcement actions with demographic breakdowns.</li> <li>● Ensure whistleblower protections for those reporting OSA misuse.</li> <li>● Enable public interest litigation provisions allowing civil society to challenge OSA applications and mandate consideration of international human rights jurisprudence in all OSA cases.</li> </ul>
Human Rights Impact Assessments	<ul style="list-style-type: none"> <li>● Ensure strict application of the three-part test (legality, legitimacy, necessity/proportionality) for all restrictions. GNI's extensive <a href="#">experience</a> in human rights due diligence, along with its robust <a href="#">tools and resources</a> – such as the <a href="#">Content Regulation and Human Rights Policy Brief</a> – can provide critical guidance in designing and implementing effective assessment frameworks.</li> <li>● Include affirmative obligations to actively promote free expression, not solely to impose restrictions, and establish regular review mechanisms with inclusive participation from diverse stakeholder groups, including civil society.</li> </ul>
Procedural Safeguards	<ul style="list-style-type: none"> <li>● Mandate public consultation periods of at least six months for any amendments and require parliamentary supermajority for OSA-related legislation.</li> <li>● Require independent multistakeholder post-enactment</li> </ul>

	review after one year of implementation.
--	--

In addition to the specific concerns and recommendations outlined above, GNI also notes with concern the overbroad definition of “intermediary” in the OSA, which imposes blanket obligations across a wide range of online services. This approach risks creating disproportionate compliance burdens, particularly for small and medium-sized enterprises, and may hinder innovation and competition in Sri Lanka’s digital ecosystem. Regulatory obligations should be appropriately tailored to a service’s function, reach, and risk profile. We also emphasize the absence of adequate mechanisms for user remedy and redress, which are essential to ensuring due process and accountability when content is restricted or removed.

GNI encourages the Government of Sri Lanka to continue its engagement with all relevant stakeholders in a broad, transparent, and inclusive manner. Robust multistakeholder consultation is critical to ensuring that any legislative reform aligns with Sri Lanka’s constitutional guarantees and international human rights commitments, while effectively addressing genuine concerns related to online safety. Please let us know if we can be of further assistance in providing additional analysis or recommendations, or by helping to convene relevant civil society and private sector experts to engage on the OSA.

### ***About GNI***

GNI brings together more than 100 prominent academics, civil society organizations, information and communications technology (ICT) companies, and investors from around the world. Over the last several years, GNI has reviewed, commented on, and helped shape a range of “[online safety](#)” bills across several jurisdictions. Our human rights analysis and recommendations for policymakers can be found in the [Content Regulation & Human Rights Policy Brief](#), which uses international human rights principles to analyze a wide range of legislative efforts and provides proactive guidance on how to address online safety in a rights-protective manner. These recommendations draw on that Brief and readers are referred to it for more detailed analysis.