PRESS STATEMENT ON THE ONLINE SAFETY BILL 2024

FOR IMMEDIATE RELEASE
11 December 2024

ARTICLE 19 and the Centre for Independent Journalism (CIJ) are concerned about some specific provisions of the Online Safety Bill (OSB) 2024, tabled in Parliament yesterday for the first reading due to the Bill's strong potential to undermine freedom of expression in Malaysia.

ARTICLE 19 and the CIJ, as part of the Expert Council formed by the Minister of Law and Institutional Reform in August this year, submitted our concerns and recommendations based on the parameters presented by the government in September 2024.

We recognise the need to hold online service providers and social media platforms accountable where their products and services have a profound negative impact on human rights. While not all are identical, the business models of the largest platforms often rely on data-driven advertising, data monetisation, and algorithms that prioritise user engagement. This can lead to detrimental consequences due to incentivising harmful content through algorithmic amplification that prioritises high engagement generating content, amplifying misleading, sensational and inciting speech as it provokes strong emotions and increases engagement. The priority of the platforms to favour profits over human rights disrupts user exposure to diverse voices and viewpoints, thus undermining democracy, freedom of expression, equality, and diversity.

We welcome a few aspects of the Bill, namely that, according to Section 2(2), it does not apply to the private messaging feature of any applications service and content applications service. We also acknowledge that the Bill states that users' freedom of expression shall not be limited unreasonably and disproportionately under Section 13(3).

However, many aspects of the Bill pose significant risks to freedom of expression, undermining the effectiveness of the protections in Section 13. We would like to reiterate our positions and convey our disappointment that some of our recommendations are not reflected in the proposed Bill, especially concerning the regulatory powers given to the Minister of Communications and the Malaysian Communications and Multimedia Commission (MCMC).

We stress that any regulation of an Application Service Provider (ASP), Content Application Service Provider (CASP) and Network Service Provider (NSP) must prioritise transparency and ensure that it strengthens, not undermines, freedom of expression and human rights. The OSB does not adequately incorporate these essential principles, crucial for maintaining an open and democratic online environment.

Key freedom of expression concerns raised by the OSB

The following provisions of the OSB undermine good governance and accountability and violate freedom of expression:

1. **Lack of an independent oversight body - The Malaysian Communications and Multimedia Commission (MCMC) is not independent and is granted excessively broad powers.**

Any legislation regulating online platforms should be overseen by an independent body with sufficient safeguards for its independence and expertise, including regarding freedom of expression. The protection of human rights should be at the center of any regulation of social media companies.

This OSB's substance is highly compromised as the regulatory powers are conferred to the Minister of Communications and the MCMC. It is tied to the powers of the Minister and the MCMC contained in the Communications and Multimedia Act (CMA), which includes the powers added in the amendments passed in Parliament on 9 December 2024.

The Minister's authority - broadened under Sections 35, 74, 80 and 81 of the OSB, amongst others - would enable the Minister to direct "authorised officers" to intercept, record and install devices for surveillance and investigation without the necessary safeguards. The powers to adopt subsidiary legislation under the OSB further remove the power of the Parliament to scrutinise and provide the necessary checks and balances. The powers of the Minister concerning the MCMC Act are further challenged in the tabling of the second reading of the amendments to the MCMC Act, resulting in it being referred to the Parliamentary Special Select Committees (PSSCs).

As a regulator, the MCMC is not independent in law and practice and has unfettered power, which is detrimental shown as follows:

- Based on their track record, the MCMC lacks the expertise to carry out the responsibilities provided under this OSB, like being unable to identify and differentiate between lawful and illegal content.
- There is a serious possibility of government or political interference as the MCMC receives directions from the Minister of Communications on exercising their powers, functions and duties, whether of a general character or "otherwise" under Section 7 of the CMA.
- OSB was tabled after the CMA amendments were passed in Parliament on 9 December 2024. These CMA amendments significantly expanded the powers of MCMC, empowering and granting them unfettered authority to monitor, investigate, and regulate the online environment. Similar functions and powers have been given to the MCMC as a regulator under the OSB, including:
    - **Section 30(1):** the power to issue directions to service providers
    - **Sections 54, 55 and 56:** grant power to an authorised officer the power to search and seize information from service providers, including without warrant and safeguards under Sections 116 and 116A of the Criminal Procedure Code (Act 593), violating privacy and due process rights;
    - **Section 57:** any authorised officer shall again be given access to computerised data without judicial oversight.
    - **Sections 60 and 61:** allow officers to order the preservation and forced disclosure of user data/communications data through a notice in writing so long as the officer is 'satisfied' that the data is 'reasonably required for an investigation' and believes there is a risk of the data becoming inaccessible and destroyed. These provisions do not require prior judicial notice or review. These sections are highly problematic given the obligation to preserve and disclose communications data, which only requires a notice in writing without any judicial oversight, and any authorised officer can request communication data.

- Further, the Online Safety Committee shall advise and give recommendations to the MCMC. It is positive that its membership is open to various stakeholders, including representatives of the disabled and those with expertise. However, it only serves to advise and give recommendations, limiting its power and impact. The power to issue instructions regarding compliance with the Act still rests in the hands of MCMC (Part V of the Bill).

- Therefore, we propose that the oversight of the OSB be delinked from the CMA and MCMC and, instead, establish a separate and new **independent Online Safety Commission** that is free from government interference as an effective regulatory body and accountability mechanisms.

2. Overreach of the Online Safety Appeal Tribunal

The establishment of Online Safety Appeal Tribunal under Section 40, on the surface appears as providing the necessary due process and the right to be heard. However,

Section 48(2) grants the Tribunal the power to determine 'affirmation and punishment for contempt'. The authority to sit in and make decisions regarding proceedings of contempt of court are vested exclusively in the courts. No individual, entity, or institution other than the court itself may sit in and decide on such proceedings. The overreach of the powers would usurp the role of the courts.

3. Broad and vague list of different types of "harmful content"

The reference to "harmful" content under the First Schedule [Section 4] suggests that this can include content that is not illegal but instead "legal but harmful". We note in particular that with the exception of content on child sexual abuse material as provided for under section 4 of the Sexual Offences against Children Act 2017 [Act 792]), the other types of content are broad and not defined clearly.

- This will likely result in increased 'lawful content' being taken down from the internet. We also see a risk that this opens the door for the government to exploit or manipulate companies' content moderation systems to censor unwanted speech (for example, by political opponents or social movements that are critical of those in power).
- It also appears that Application Service Providers (ASP), Content Application Service Providers (CASP) and Network Service Providers are expected to proactively screen or filter their users' content and prevent the public from seeing anything deemed "harmful content". This amounts to prior censorship and undermines freedom of expression.
- The "harmful content", if not clearly defined, would make it difficult to enforce, prone to abuse, and open to challenge on legal grounds.
- The list of harmful content in the First Schedule from **2 to 9** would require general monitoring by ASP, CASP and NSP. Further, it is highly contentious to introduce broad and subjective content such as "obscene content" (paragraph 3), indecent content (paragraph 4), content that may incite violence or terrorism (paragraph 6), content that may promote feelings of ill-will or hostility (paragraph 8) and content that promotes the use or sale of dangerous drugs (paragraph 9), as this is likely to result in increased lawful content being taken down from the internet and lead to extensive censorship.
- As the MCMC will be the regulator of this Act, the long list of "harmful content" without a clear definition opens the room for MCMC to use the OSB to remove or filter contents. This also means that MCMC will be in a position to impose an obligation of general proactive monitoring or filtering of content by service providers under the guise of a duty of care or safety by design premise. As stated by the Special Rapporteur on FOE, this is inconsistent with the right to privacy and likely amounts to pre-publication censorship.
- Although monitoring enables companies to detect potentially illegal or other problematic content, in practice, mere detection is almost always coupled with removal or other types of actions reducing the availability of such content. This is deeply problematic, given that content-monitoring technology is not nearly as

advanced as is sometimes perceived by users. In particular, hash-matching algorithms and natural language processing tools are currently incapable - especially in the context of multilingual countries such as Malaysia - of distinguishing content whose legality may vary depending on the context, such as news reporting, satire or parody. Vast amounts of legitimate content may, therefore, be removed. Moreover, these technologies interfere with users' privacy rights, as they require analysis of individuals' communications.

- This will inadvertently undermine freedom of expression as protected under Article 10(1)(a) of the Federal Constitution. It is well noted that freedom of expression is not absolute, and, under the Federal Constitution, it is subject to restrictions deemed necessary or expedient through an act of law passed by Parliament.
- The above broad definitions of categories of harmful content are not in line with the three-part test, particularly the principle of legality, which requires that the law be formulated with sufficient precision to enable individuals to regulate their conduct. Under Article 19(3) of the ICCPR, restrictions to the freedom of expression are permissible only when "provided by law" and necessary for "the rights or reputations of others" or "for the protection of national security or of public order or public health and morals". Legality, legitimacy, necessity and proportionality under Article 19(3) of the ICCPR should be applied throughout the OSB to align with freedom of expression standards.[1]

4. The Duties of Licensed Application Service Provider (ASP) and Content Application Service Provider (CASP).

There is a risk that the duty of care principle is used to over-moderate and undermine freedom of expression.

- Under Section 13(3), we note that the Bill is mindful that users' expression shall not be limited unreasonably and disproportionately through the measures being implemented. Yet, such a provision is insufficient to offer meaningful protection as, at the onset, the powers to remove content and the non-compliance threshold are against freedom of expression standards. It is also unclear what measures will be used to determine compliance with the requirements under Section 13(3).

5. Liability of Licensed Application Service Provider (ASP) and Content Application Service Provider (CASP).

Given the OSB's main focus on requiring ASP and CASP to reduce certain types of "content," – coupled with the financial penalty the OSB provides for non-compliance - it will inadvertently provide ASP and CASP with a strong incentive to over-censor their

[1] Though Malaysia is not a party to the ICCPR, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted in 2018 that the content of Article 19 of the ICCPR is based on Article 19 of the Universal Declaration on Human Rights (UDHR) and thus should inform Malaysia's obligations under international law.

users to limit their liability exposure. This is particularly true given the vague concepts and definitions like “harmful” content.

6. **The failure to address the underlying issues within a systems-based approach**

The OSB's objectives should not be limited to tackling illegal content, much less “harmful” content, as this concept is too broad. Instead, we stress that any regulation of online service providers must be located within its systems and processes, and prioritise transparency, accountability, and the protection of human rights.

The prior consultations initiated by the government created the impression that the OSB would focus on a system-based approach. However, large sections of the OSB are highly focused on content moderation and making content inaccessible. The content-focus approach ignores systemic problems by focusing on symptoms (“harmful content”) rather than the underlying or root causes, which could include platform design flaws, the use of algorithms to amplify content, or a lack of user education. There is also a high risk of surveillance and impact on privacy as giving ASP and CASP more authority to carry out moderation tasks may result in platforms collecting, storing, analysing, and researching user behaviour patterns in an excessively broad manner.

A system-based approach should focus on the design, governance and operational processes of ASP and CASP rather than a focus on specific “harmful content”. The service providers should be required to put systems and processes in place to protect human rights, prevent harm and mitigate risks, including empowering users, ensuring algorithmic transparency and adopting safety-by-design features.

Recommendations

The aspects highlighted here represent just a few of the many issues in the OSB, if unaddressed, would fail to ensure users' online safety. Overall, we find the Bill flawed in its approach, with the potential to undermine rather than protect human rights online. Therefore, we urge legislators to overhaul the Bill and carefully consider and address the key concerns we raised in this preliminary analysis and in our previous recommendation.

In particular, we recommend that the government and Members of Parliament:

1. Halt the subsequent reading and refer the OSB to the Parliamentary Special Select Committee on Human Rights, Elections, and Institutional Reform for further review and consultation.
2. Establish an independent Online Safety Commission free from government interference as an effective regulatory body and accountability mechanism.

3. Ensure that the OSB is brought in line with freedom of expression standards, respecting the principles of legality, legitimacy, necessity and proportionality throughout.