ASIA
INTERNET
COALITION

28 April 2023

Mr Lew Chuen Hong
Chief Executive
Infocomm Media Development Authority
10 Pasir Panjang Rd,
#03-01 Mapletree Business City, Singapore 117438

Dear Lew Chuen Hong,

Asia Internet Coalition (AIC) Comments on IMDA's Draft Code of Practice for Online Safety

The Asia Internet Coalition (AIC) and its members express our sincere gratitude to the Infocomm Media Development Authority (IMDA) for the opportunity to submit comments on the Draft Code of Practice for Online Safety.

The AIC is an industry association of leading Internet and technology companies. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region. Our member companies would like to assure the IMDA that they will continue to actively contribute to online safety on digital platforms, products and services in support of the digital economy goals of Singapore.

We commend IMDA for its efforts in drafting the Code of Practice for Online Safety for designated Social Media Services to help improve Singapore's online safety regulatory framework. While we support these efforts, we also wish to express our concerns about some of the requirements proposed in the draft code. As such, please find attached to this letter detailed comments and recommendations, which we would like the IMDA to consider when preparing the final code.

We are grateful to the IMDA for upholding a transparent, multi-stakeholder approach in developing the Code of Practice for Online Safety. We further welcome the opportunity to offer our inputs and insights, directly through meetings and participating in the official consultations once the final draft of codes is available for comment.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490.

Thank you
Sincerely,

Paine

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Detailed Comments
Code of Practice for Online Safety

Section A: Overall

We seek to understand the reasons for the paragraphs that were added to the latest draft of the Code of Practice for Online Safety, which recommends significantly higher responsibilities on designated social media services to proactively detect and remove harmful content. The earlier draft circulated as part of the public consultation recommended a more collaborative and outcomes-based approach to content moderation that relied on the combination of user reporting and government notice and takedown mechanisms that would effectively help identify and remove harmful online content that affects users in Singapore.

We recommend that the IMDA adopt a less prescriptive approach to the drafting of the Code of Practice for Online Safety, similar to the earlier draft of the Code that was circulated as part of the public consultation.

1. For example, allowing users to submit requests to social media services for a review of the decision and action taken on reported content deviates from the earlier Ministry of Communications and Information (MCI)'s agreement in their Summary of Responses to the Public consultation with the industry on the need to adopt an outcome-based approach towards enhancing online safety.
2. Requiring designated services to respond to every user request for review of a decision and action taken regarding reported harmful content places significant resource strains on services, impacts the efficiency of services to prioritize and process complaints effectively, and takes away resources and time that could be channelled towards more pressing content issues such as those involving child sexual abuse material and terrorism content.
3. We recommend that such onerous user reporting and resolution requirements be removed from the Code.

We strongly recommend IMDA to conduct another round of industry consultation on the latest draft of the Code of Practice for Online Safety, and the forthcoming draft of the Content Code for Social Media Services.

We also request greater clarity on how IMDA intends to implement the Bill provisions on the Codes of Practice for Online Safety, should Parliament approve the Bill.

Given the interest in the public for MCI and IMDA to look into other potential areas of concern, we would also like to seek IMDA's assurance that the Code of Practice for Online Safety will be limited to the scope of social media services only. Any interest to regulate other types of digital content should be accompanied by a robust industry consultation process and separate codes of practice and accompanying legislation.

1. Community guidelines and standards and content moderation

11. Users' exposure to harmful content must be minimized via reasonable and proportionate measures. These measures include, but are not limited to, a set of community guidelines and standards, and content moderation measures that are put in place and effected by the Service. The Service's community guidelines and standards must address the categories of harmful content in paragraph 4 and must be published.

AIC Feedback:

We support the recommendation of relying on a set of community guidelines to limit users' exposure to harmful content. However, each designated social media service has its own individual risk assessments on what would constitute harmful content and be taken down. Such proactive general monitoring obligations place significant resource burdens on designated social media services and potentially create a disparate approach towards improving online safety across services.

A clear distinction should also be made between what material is deemed as "illegal" and should be removed, and content that is "legal but harmful" that should be subject to clear and transparent policies. We recommend that the Government play a key role in collaborating with designated social media services to identify what material is illegal and harmful that needs removing, for example through formal notice and takedown schemes.

We also suggest that the Ministry provides illustrative but non-exhaustive examples of categories of Harmful Content to avoid broad scope of the implementation of this Code.

This feedback also applies to Para 17.

2. Empower users and improve safety

13. Users must be able to easily access information related to online safety on the Service. Such information must be easy to understand and must include the availability of tools and local information, including Singapore-based safety resources or support centres, if available. The Service should seek to implement, support and/or maintain programmes and initiatives to educate and raise awareness of such information.

14. Users who use high-risk search terms such as, but not limited to, terms relating to self-harm and suicide on the Service must be actively offered relevant safety information (stated in paragraph 13) such as, but not limited to, local suicide prevention hotlines, if available.

AIC Feedback:

We support the recommendation that Singapore-based safety resources and information be made easily accessible to users. While social media services will make their best efforts to support the government's recommendations, we would like to highlight that there is a tendency for users to mask their geo-location during their use of social media services. This limits the ability of social media services to push such important local information to such users. We recommend that social media services not be held liable in such instances where a user makes a conscious effort to mask their geo-location while using the service.

We recommend encouraging IMDA to provide examples to illustrate their expectation here; we'd support publicising such resources and working together with IMDA to achieve this outcome. IMDA should allow platforms to decide based on their best judgment. Otherwise, the high risk search terms should be provided.

We also strongly recommend that the Government work with industry to develop and maintain a “high-risk search terms” list and a list of sites to which users should be redirected.

This feedback also applies to Para 22.

3. Proactive detection and removal

15. Users' exposure to child sexual exploitation and abuse material and terrorism content on the Service must be minimised through the use of technologies and processes. These technologies and processes must proactively detect and swiftly remove child sexual exploitation and abuse material and terrorism content as technically feasible, such that the extent and length of time to which such content is available on the Service is minimised.

16. Users must be protected from child sexual exploitation and abuse activity and terrorism activity on the Service through reasonable and proportionate steps taken by the Service to proactively detect and swiftly remove preparatory child sexual exploitation and abuse activity (such as online grooming for child sexual abuse) and terrorism activity (such as glamourising or endorsing terrorist activities).

AIC Feedback:

Technologies and processes that target child sexual abuse material and terrorism content are supported by referencing hash databases of existing material. In this regard, current technological solutions are limited in what they can reasonably detect. Similarly, there remain significant limitations on existing detection technologies related to online grooming and terrorism activity.

Such technology limitations should be taken into account in the government's application of the Code in reference to the Online Safety Bill.

Global hash databases of known child sexual abuse material and terrorism content are predominantly focused on Caucasian children from the US and the EU, and greater public-private sector partnership is required to “train” these databases to detect such material from other regions including Asia.

We recommend that the government spearhead collaboration between the community, including NGOs, and the private sector to build up the hash databases of known child sexual abuse material and terrorism content to improve the ability of services to proactively detect and remove such material using technology.

We also recommend that the government adopt a “Proactive disrupt and deter” approach as detection only limits the options that providers can use to show they are protecting kids to only a few technologies. A “disrupt and deter” approach allows companies the flexibility to, for instance, use patterns of behaviour to kick bad actors off systems even if you cannot actually see CSAM images.

We seek clarity on what qualifies as terrorism. There should be a list of terrorist groups IMDA can provide, such as the Local Terrorist Organisation list for Singapore. IMDA also should clarify if terrorism content is being referred to extra-territorial or just limited to occuring in Singapore?

We also seek clarity on how IMDA defines “grooming” and “communication with the intent to radicalize”. The reason being that grooming or “glamourising or endorsing terrorist activities” can come in a multitude of forms and can start with relatively common interactions.

Section B: Measures for children

1. Community guidelines and standards and content moderation

18. Children must not be targeted to receive content that the Service is reasonably aware to be detrimental to their physical or mental well-being. Such content includes the categories of harmful and/or inappropriate content in paragraphs 4 and 17. In this regard, content targeting refers, but is not limited to, advertisements, promoted content and content recommendations.

AIC Feedback:

We support the recommendation that children should not be targeted to receive content that is detrimental to their physical or mental well-being. However, we would like to highlight that there are tendencies for young users to provide false information about their age, which limits the ability of social media services to prevent such content targeting. In this regard, such age-gating or age-assurance techniques have had limited success in restricting digital content from children. Further, “inappropriate content” is too broad.

2. Protection for children

20. Unless the Service restricts access by children, children must be provided differentiated accounts whereby the settings for the tools to minimise exposure and mitigate impact of harmful and/or inappropriate content and unwanted interactions are robust and set to more restrictive levels that are age appropriate by default. Children or their parents/guardians must be provided clear warnings of implications if they opt out of the default settings.

AIC Feedback:

We support the recommendation that designated social media services that allow users below 18 to have optional child settings as an additional safeguard for young users. However, we recommend that any requirements should not be prescriptive to allow designated social media services the flexibility to develop and implement the most appropriate solutions to tackle harmful online content on their services, taking into account their unique operating models.

Section C – User Reporting and Resolution

23b. Where the Service receives a report that is not frivolous or vexatious:

I. The user who submitted the report must be informed of the Service's decision and action taken with respect to that report without undue delay.
II. Should the Service decide to take action against the reported content or account(s), the user holding the account(s) that generated, uploaded, or shared the reported content must be informed of the Service's decision and action without undue delay.

c. The users referred to in sub-paragraphs (b)(i) and (b)(ii) must be allowed to submit requests to the Service for a review of the decision and action taken.

AIC Feedback:

Requirements for designated services to respond to every user request for review of a decision and action taken regarding reported harmful content places are not necessary to prevent or address the harms involved, and would put a significant on resources, at the expense of more urgent priorities (e.g. the actual takedown obligations).

We strongly recommend that such onerous individual user reporting and resolution requirements be removed from the Code. In terms of reporting, the annual reports to IMDA as required by Para 25 are a more proportionate reporting measure.

25. In this regard, the Service must submit to IMDA annual reports on the measures the Service has put in place to combat harmful and inappropriate content, for publishing on IMDA's website. The annual reports should reflect Singapore users' experience on the Service, including:

a. How much and what types of harmful or inappropriate content they encounter on the Service;
b. What steps the Service has taken to mitigate Singapore users' exposure to harmful or inappropriate content; and
c. What action(s) the Service has taken on user reports.

AIC Feedback:

The intent of para 25 is for Services to report on the amount of harmful content that has been moderated. We would like to seek greater clarity on the need for annual reports to reflect Singapore users' experience of the Service, as this additional requirement would be unnecessarily burdensome and unhelpful towards the original intent. For example, companies would have to conduct regular interviews with their users just to complete the section on the user's experience of the service.