

Technology, Media & Telecommunications

Measures to Enhance Online Safety – Singapore Introduces New Legislation

Introduction

Singapore has been making concerted efforts towards enhancing the safety of digital spaces for Singapore users, particularly for children. This is in recognition of the inherent risks posed by harmful online content, and the amplification of such risks through the proliferation of social media services.

The Ministry of Communications and Information ("**MCI**") had, earlier in 2022, given an indication of what changes and enhancements may be expected in the digital regulatory and compliance framework, including the introduction of codes of practice for online platforms to protect Singaporeans against harmful online content. The proposed measures have been steadily advancing along the course of implementation, and are now being further developed, with new legislation being introduced in Parliament, and responses to public feedback on the proposed measures.

From 13 July 2022 to 10 August 2022, MCI conducted a Public Consultation on Proposed Measures to Enhance Online Safety for Users in Singapore ("**Public Consultation**"). For more information, please see our earlier Legal Update on this topic [here](#). On 29 September 2022, MCI released a summary of its responses to the feedback received from the Public Consultation, giving further indication of the direction that the proposed measures may take.

On 3 October 2022, the Online Safety (Miscellaneous Amendments) Bill ("**Bill**") was introduced in Parliament. If passed, the Bill will empower the Infocomm Media Development Authority ("**IMDA**") to better regulate online communication services accessible by Singapore end-users and give effect to the proposed measures, including the authority to issue directions to block egregious content and to issue online Codes of Practice.

This Update highlights the key provisions in the Bill and provides a summary of the feedback to the Public Consultation.

Online Safety (Miscellaneous Amendments) Bill

The Bill had its First Reading in Parliament on 3 October 2022 and is set for its Second Reading at the first available sitting in November 2022. The Bill seeks to provide a safe online environment for Singapore end-users, and to place adequate priority on the protection of children from exposure to harmful content.

Technology, Media & Telecommunications

The main proposed amendment in the Bill is the introduction of a new Part 10A in the Broadcasting Act 1994. Part 10A aims to give effect to the proposed measures for enhancing online safety by:

- (a) Allowing IMDA to issue blocking directions to online communication services to deal with "egregious content"; and
- (b) Empowering IMDA to issue online Codes of Practice for providers of regulated online communication service.

An online communication service includes such service provided from outside Singapore, as well as such service provided in or from Singapore. The list of online communication services is presently limited to social media services under the proposed new Fourth Schedule of the Broadcasting Act. However, the Minister may, by order in the Gazette, revoke, replace or add to the Fourth Schedule.

Blocking Directions

IMDA may issue the following directions under the proposed Part 10A:

- (a) **Section 45H direction** – IMDA may issue a section 45H direction to the provider of an online communication service to:
 - Disable access to egregious content on its service by Singapore end-users; or
 - Stop delivery or communication of content to the account(s) (such as a social media account, group or channel) of all Singapore end-users (or a sub-group) so as to stop or reduce the communication, provision or access by Singapore end-users of the egregious content on the online communication service.

This is provided that IMDA is satisfied that egregious content is being provided on the online communication service with a Singapore end-user link, and that Singapore end-users of the service can access the egregious content. It also does not apply to communication between two or more end-users that is of a private or domestic nature.

- (b) **Section 45I blocking direction** – IMDA may issue a section 45I blocking direction to an internet access service provider to stop access by Singapore end-users to the online communication service.

This would occur when an online communication service provider fails to comply with a section 45H direction, and the internet access service provider has control over access by Singapore end-users of the online communication service to content provided on that online communication service.

The Bill provides further guidance on what may constitute egregious content, including content advocating suicide or self-harm, physical or sexual violence and terrorism, content depicting child sexual

Technology, Media & Telecommunications

exploitation, content posing a public health risk in Singapore, and content likely to cause racial and religious disharmony in Singapore.

Every provider of an online communication service or an internet access service who receives a section 45H direction or a section 45I blocking direction respectively has a duty to take all reasonably practicable steps to comply with the direction.

- (a) Section 45E: Failure to satisfy this duty with regard to a section 45H direction may result in a fine not exceeding S\$1 million and, in the case of a continuing offence, a further fine not exceeding S\$100,000 for every day or part of a day during which the offence continues after conviction.
- (b) Section 45F: Failure to satisfy this duty with regard to a section 45I blocking direction may result in a fine not exceeding S\$20,000 for each day or part of a day the person does not comply with the direction, subject to a total cap of S\$500,000.

It does not matter whether the online communication service is provided from outside Singapore or provided in or from Singapore.

The Bill provides a defence for the breach of the above duty, in which the person charged must prove that:

- (a) It was not reasonably practicable to do more than what was in fact done to satisfy the relevant duty; and
- (b) There was no better practicable means than was in fact used to satisfy the relevant duty.

A section 45H direction or a section 45I blocking direction is appealable to the Minister.

Codes of Practice

IMDA may designate an online communication service with a Singapore end-user link as a regulated online communication service after considering the range of all online communication services provided to Singapore end-users, and the extent and nature of their effect on the people of Singapore and her different communities.

The new section 45L of the proposed Part 10A empowers IMDA to issue online Codes of Practice applicable to providers of any regulated online communication service or specified types of such providers. However, an online Code of Practice can only be issued, amended or revoked after certain consultation processes are followed.

Technology, Media & Telecommunications

A Code of Practice may provide for the following:

- (a) **Measures to minimise risk** – Requirements to establish and apply appropriate systems or processes so as to provide the service in a way that: (i) prevents users (particularly children) from accessing content that presents a material risk of significant harm to them; and (ii) mitigates and manages the risks of danger to users (particularly children) from content on its service;
- (b) **Guidance on risk** – Practical guidance in respect of what content presents a material risk of significant harm;
- (c) **Procedure for compliance** – The procedures to be followed to satisfy the duty to comply with the online Code of Practice applicable to that provider, which may include: (i) audit to ascertain compliance; (ii) reporting to IMDA information about the measures taken; and (iii) conducting risk assessments on the systemic risks of their services and taking reasonable and effective measures aimed at mitigating those risks.
- (d) **Collaboration with research** – Requirements for collaboration or cooperation by the provider with any conduct of research into its regulated online communication service by a suitable expert.

The Bill imposes a duty on every regulated online communication service provider to take all reasonably practicable steps to comply with the applicable online Code of Practice in the provision of the regulated online communication service. A defaulting provider may face the following regulatory action from IMDA under the proposed section 45N:

- (a) An order to pay a financial penalty that IMDA thinks fit, but not exceeding S\$1 million; or
- (b) Directions to take any steps that may be necessary to remedy the failure. If a defaulting provider fails to comply with the remedial directions, the defaulting provider may be liable to a fine not exceeding S\$1 million and, in the case of a continuing offence, to a further fine not exceeding S\$100,000 for every day or part of a day during which the offence continues after conviction.

Similar to the provisions on blocking directions, it is a defence for the defaulting provider to prove that:

- (a) It was not reasonably practicable to do more than what was in fact done to satisfy the relevant duty; and
- (b) There was no better practicable means than was in fact used to satisfy the relevant duty.

Amendments will be made to the Electronic Transactions Act 2010 to expressly clarify that the safe harbour provisions under the Electronic Transactions Act for network service providers does not apply in relation to any liability under sections 45E, 45F or 45N of the amended Broadcasting Act.

Technology, Media & Telecommunications

Response to Public Consultation

From 13 July 2022 to 10 August 2022, MCI conducted the Public Consultation, which set out the proposed measures to address harmful online content on social media services:

- (a) **Code of Practice for Online Safety**, which sets out the required measures and safeguards against harmful content to be implemented by designated social media services; and
- (b) **Content Code for Social Media Services**, which empowers IMDA to direct social media services to disable access to harmful content.

On 29 September 2022, MCI issued a summary of the key feedback received, and MCI's response to the feedback. MCI indicated that overall, respondents were supportive of the proposed measures. Some of the key feedback and responses are highlighted below.

1. Systems and processes for designated social media services

Feedback: Respondents generally agreed with the proposal for designated social media services to have appropriate systems and processes to reduce exposure to harmful online content. Some respondents highlighted other areas of concern, such as harmful advertisements, online gaming, scams, misinformation and online impersonation. Some respondents suggested that penalties be imposed for non-compliance, while others sought assurance that the proposed measures would not affect user privacy or freedom of expression.

Industry groups suggested an outcome-based approach in regulating social media services, which takes into account for example, their business models and size in implementing the proposed requirements. They also sought clarity on how designated services would be identified and defined.

Response: MCI indicated that its priority is to address harmful online content on designated social media services for this round of measures, but that they will continue to study the other areas of concern raised. MCI acknowledged that it would need to find the right balance between prioritising user safety and managing privacy and freedom of expression.

MCI agreed on the need to adopt an outcome-based approach and indicated that designated social media services will be given some flexibility to develop and implement the most appropriate solutions to tackle harmful online content on their services, taking into account their unique operating models.

Technology, Media & Telecommunications

2. Safety features and tools to manage exposure

Feedback: Respondents generally agreed with the importance of having safety features and tools on social media services to allow users to manage their exposure to harmful online content. Many respondents were not aware of existing safety features and felt that more could be done by social media services to raise user awareness and usage.

Response: MCI indicated that it encourages social media services to step up their efforts to raise users' awareness of the safety features available on their services, and to convey information on self-help resources to users. MCI also stated that it will continue to work with other Government agencies and community partners to enhance public education efforts on online safety.

3. Additional safeguards to protect young users

Feedback: Respondents were supportive of the proposal for designated social media services to have additional safeguards for young users. Industry groups suggested adopting an outcome-based approach when implementing safeguards for young users.

Response: MCI acknowledged that social media services differ in terms of their user profiles and the type of content published on their services. MCI indicated that it would continue to work with the industry to study the feasibility of the suggestions to apply an outcome-based approach to improving the safety of young users on these services.

4. User reporting mechanism on social media services

Feedback: Most respondents supported the proposal for social media services to have an effective user reporting and resolution process, and to release annual reports on the effectiveness of their content moderation policies and practices to combat harmful content.

Response: MCI agreed that designated social media services should have an accessible, effective, and easy-to-use user reporting mechanism. Designated social media services should also submit annual accountability reports on the effectiveness of their measures to combat harmful content, which are to be made public.

5. Blocking directions to social media services to disable access to egregious content

Feedback: For the proposal that IMDA be empowered to issue directions to social media services to block egregious content, respondents and industry groups suggested that explanations should be provided on why the specific content was deemed harmful. Industry groups also suggested that social media services be given some flexibility on the timelines for such content to be removed, taking into account the severity of the harmful content and the resources of the service.

Technology, Media & Telecommunications

Response: MCI clarified that, when issuing blocking directions to social media services, the egregious content of concern would be made clear to the services. MCI also provided that the timeline requirements for social media services to comply with the directions would take into account the need to mitigate users' exposure to the spread of egregious content circulating on the services.

6. Collaboration between community, private sector and Government

Feedback: Most respondents recognised the importance of public education to guide users in dealing with harmful online content and engaging with other users online in a safe and respectful manner. Many respondents suggested that the Government could tap on school and parent/peer networks for public education and outreach to parents and young users, and that the community could partner the Government and industry to raise awareness of existing resources.

Response: MCI agreed that online safety regulations need to be complemented by effective public and user education. MCI highlighted that the Government has launched public education programmes to impart digital media and information literacy and cybersecurity skills. MCI also welcomed the participation of the community and industry in making online spaces safer.

Concluding Words

The proposed measures to enhance online safety are progressing steadily towards implementation, with public feedback having been considered and legislation being introduced. It is expected that the Government will continue to push forward with these measures to achieve effective implementation. The IMDA website (available [here](#)) states that it expects to bring the proposed Codes of Practice into force in the second half of 2023.

It should be noted that the proposed Codes of Practice and the blocking directions that IMDA may be empowered to issue will impose a wide scope of obligations on the part of social media services and related service providers such as internet access service providers. The introduction of the corresponding penalties, such as fines and imprisonment, indicate that the breach of these obligations will have potentially serious implications on the relevant service providers.

Importantly, the proposed changes would apply to all online communication services that can be accessed by Singapore end-users, and would extend to services provided from outside Singapore.

Organisations in the industry should thus familiarise themselves with the proposed framework for online safety and ensure that they comply with the relevant obligations by implementing the necessary measures and safeguards.

The full Summary of Responses to Public Consultation on Enhancing Online Safety for Users in Singapore is available [here](#).

Technology, Media & Telecommunications

For further queries, please feel free to contact our team below.

Contacts



Rajesh Sreenivasan
Head, Technology, Media &
Telecommunications

T +65 6232 0751

rajesh@rajahtann.com



Steve Tan
Deputy Head, Technology,
Media & Telecommunications

T +65 6232 0786

steve.tan@rajahtann.com



Benjamin Cheong
Deputy Head, Technology, Media
& Telecommunications

T +65 6232 0738

benjamin.cheong@rajahtann.com



Lionel Tan
Partner, Technology, Media &
Telecommunications

T +65 6232 0752

lionel.tan@rajahtann.com



Tanya Tang
Partner (Chief Economic and
Policy Advisor), Technology,
Media & Telecommunications

T +65 6232 0298

tanya.tang@rajahtann.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

Our Regional Contacts

RAJAH & TANN | *Singapore*

Rajah & Tann Singapore LLP

T +65 6535 3600
sg.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*

Christopher & Lee Ong

T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

R&T SOK & HENG | *Cambodia*

R&T Sok & Heng Law Office

T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN | *Myanmar*

Rajah & Tann Myanmar Company Limited

T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

RAJAH & TANN 立杰上海

SHANGHAI REPRESENTATIVE OFFICE | *China*

**Rajah & Tann Singapore LLP
Shanghai Representative Office**

T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

GATMAYTAN YAP PATACSIL

GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*

Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)

T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*

Assegaf Hamzah & Partners

Jakarta Office

T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office

T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Thailand*

R&T Asia (Thailand) Limited

T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*

Rajah & Tann LCT Lawyers

Ho Chi Minh City Office

T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

RAJAH & TANN | *Lao PDR*

Rajah & Tann (Laos) Co., Ltd.

T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

Hanoi Office

T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Rajah & Tann Asia is a network of legal practices based in Asia.

Member firms are independently constituted and regulated in accordance with relevant local legal requirements. Services provided by a member firm are governed by the terms of engagement between the member firm and the client.

This update is solely intended to provide general information and does not provide any advice or create any relationship, whether legally binding or otherwise. Rajah & Tann Asia and its member firms do not accept, and fully disclaim, responsibility for any loss or damage which may result from accessing or relying on this update.

Client Update: Singapore

2022 OCTOBER

LAWYERS
WHO
KNOW
ASIA

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.

The contents of this Update are owned by Rajah & Tann Singapore LLP and subject to copyright protection under the laws of Singapore and, through international treaties, other countries. No part of this Update may be reproduced, licensed, sold, published, transmitted, modified, adapted, publicly displayed, broadcast (including storage in any medium by electronic means whether or not transiently for any purpose save as permitted herein) without the prior written permission of Rajah & Tann Singapore LLP.

Please note also that whilst the information in this Update is correct to the best of our knowledge and belief at the time of writing, it is only intended to provide a general guide to the subject matter and should not be treated as a substitute for specific professional advice for any particular course of action as such information may not suit your specific business and operational requirements. It is to your advantage to seek legal advice for your specific situation. In this regard, you may call the lawyer you normally deal with in Rajah & Tann Singapore LLP or email Knowledge & Risk Management at eOASIS@rajahtann.com.