

Technology, Media & Telecommunications

Online Criminal Harms Act Passed in Singapore

Introduction

On 5 July 2023, the Singapore Parliament passed the Online Criminal Harms Act ("**OCHA**"). The OCHA is aimed at online content or activity which is criminal in nature, or which is used to facilitate or abet crimes. The OCHA allows directions to be issued to online service providers, other entities, or individuals, when specified criminal offences take place. The OCHA also requires designated online services to put in place systems and processes to counter scams and malicious cyber activities.

This Update will provide an overview of the OCHA.

Key Features of the OCHA

Issuance of directions against specified offences

The ability to issue directions to restrict exposure of Singapore users to online content and activity is not new, as such features are also found under the Protection from Online Falsehoods and Manipulation Act, the Foreign Interference (Countermeasures) Act and the Broadcasting Act, to name a few.

In this regard, the OCHA empowers designated officers from various agencies to issue directions in respect of online activity for criminal offences under their agencies' purview if the designated officer:

- (a) reasonably suspects that a specified offence has been committed and that any online activity is in furtherance of the commission of the offence; or
- (b) suspects or has reason to believe that any online activity is preparatory to, or in furtherance of, the commission of a scam or malicious cyber activity offence.

"**Specified offences**" are criminal offences that affect national security, national harmony, and individual safety, and which have an online nexus, and are further specified in the First Schedule of the OCHA.

In this regard, the OCHA allows the issuance of the following directions:

- (a) **Stop communication direction:** Under the OCHA, a direction may be issued to a person who has control of the relevant material or the proprietor of the relevant location, to require the recipient to
 - (i) take all reasonable steps to remove the relevant material; (ii) stop storing, posting, providing or



Client Update: Singapore

2023 SEPTEMBER

Technology, Media & Telecommunications

transmitting any online material similar to the relevant material; or (iii) disable access to the relevant location, by a specified time.

For example, a stop communication direction may be issued to someone who posts text or images, inciting violence against people of a certain race.

- (b) **Disabling direction:** The OCHA allows the issuance of a direction to a provider of an online service to take all reasonable steps to disable access by Singapore persons to (i) any relevant material stored, posted, provided or transmitted on or through the recipient's online service; (ii) any identical copies of the relevant material stored, posted, provided or transmitted on or through the recipient's online service; or (iii) any relevant location on the recipient's online service, by a specified time.

For example, a disabling direction may be issued to an offending post or page to prevent it from reaching users in Singapore.

- (c) **Account restriction direction:** The OCHA allows the issuance of a direction to a provider of an online service to take all reasonable steps to disallow or restrict interaction between any relevant account on the recipient's online service and Singapore persons, by a specified time. "Reasonable steps" may include the termination, suspension or restriction of one or more functionalities of the online service in relation to the relevant account if this is necessary.

Account restriction directions will prevent offending accounts from interacting with persons in Singapore.

Special provisions to counter scams and malicious cyber activities

In addition to the directions discussed above, the OCHA also empowers the authorities to take a more proactive and pre-emptive approach to scams and malicious cyber activities, given their wider reach and greater potential for harm.

In this regard, law enforcement officers are empowered by the OCHA to issue the following types of proactive directions to take action once scams and malicious cyber activities are detected, even before an offence is committed:

- (a) **Access blocking direction:** The OCHA allows the issuance of a direction to a provider of an internet access service to take all reasonable steps to disable access by Singapore persons by means of the recipient's internet access service to any relevant material or relevant location, by a specified time.

For example, scammers have been known to create thousands of blank websites in advance, with domain names that resemble those of legitimate organisations. When the malicious actor is ready to strike, these blank websites are swiftly activated, populated with scam content, and pushed out to the public, who may fall prey within minutes. Access blocking directions will prevent such websites

Technology, Media & Telecommunications

from being accessed by Singapore users even before they are activated by scammers.

- (b) **App removal direction:** The OCHA also allows the issuance of a direction to a provider of an app distribution service to take all reasonable steps to stop distributing a relevant app to Singapore persons and stop enabling Singapore persons to download a relevant app, by means of the recipient's app distribution service, by a specified time.

As the name suggests, such directions can remove scam apps that are used to commit scam offences, from Singapore app storefronts and third-party app stores.

Codes of practice and implementation directives

Designated online services

The OCHA empowers a Competent Authority to designate online services that would be subject to Codes of Practice and Implementation Directives to be applied against offences in the Second Schedule of the OCHA. For now, the Second Schedule only specifies scam and malicious cyber activity offences. However, during the Second Reading of the Online Criminal Harms Bill, Mrs. Josephine Teo, Minister for Communications and Information & Second Minister for Home Affairs ("**Minister**"), also explained that the Second Schedule can be quickly populated if new classes of offences emerge which also require counter actions.

In designating online services, the Competent Authority will consider the extent and impact of the harms relating to the specified offences, the reach and projected reach in Singapore of the online service, the design and nature of the online service, and other relevant factors.

Codes of Practice

For the purposes of countering the offences specified in the Second Schedule, the Competent Authority is empowered to issue Codes of Practice to designated online services. The requirements under the Codes of Practice will be framed in terms of outcomes which designated online services must meet, to give them greater flexibility to customise their approach, depending on the nature of their service.

If a designated service provider has not complied with an applicable Code of Practice, the Competent Authority may give the provider notice to rectify the non-compliance within the permitted time.

The Codes of Practice will supersede any (i) duty of confidentiality or privacy imposed by any rule of law; or (ii) duty imposed by any contract or any rule of professional conduct, that would otherwise prevent or restrict the person from complying with the requirements.

Implementation Directives

As a complement to Codes of Practice, the OCHA also empowers the Competent Authority to issue

Technology, Media & Telecommunications

providers of designated online service with Implementation Directives, to put in place any system, process, or measure, if it is satisfied that this is necessary or expedient to address a relevant offence under the Second Schedule. Such Implementation Directives will be specific and prescriptive, and would be useful in situations where there is an urgent need to put in place a specific measure to address the proliferation of a specific scam operation.

Appeal mechanism

The OCHA also provides for appeal mechanisms. Recipients of directions or orders must first seek reconsideration from the agency that issued the direction or order. If the request is unsuccessful, they can then appeal to a specialised Reviewing Tribunal. This allows timely and efficient remedies to be delivered via an independent channel, instead of via general appeal to the courts.

Appeals against designation of online services, Codes of Practice and Implementation Directives will be heard by the Minister for Home Affairs.

Extraterritoriality

Given that perpetrators of scams and malicious cyber activities may be based overseas, the OCHA also contains provisions that allow the issuing of directions, notices, directives and orders to entities and individuals, even if they have no presence in Singapore.

If these individuals choose not to comply, further steps could be taken, such as through prosecution, or issuing orders to restrict access to the non-compliant online service to prevent the criminal activity from being accessed here. For example, an access blocking order can be issued to Internet access service providers to prevent non-compliant online services from continuing to reach users in Singapore and do them harm.

Concluding Words

As noted by the Minister in her closing remarks to the Second Reading speech, there is no silver bullet that can resolve the complexities of the online world.

However, the OCHA certainly marks an important step towards creating a safer online space for Singaporeans, and complements existing efforts to act more effectively against online criminal activities, through partnership between the people, the Government and industry.

Developments under the OCHA, in particular the Codes of Practice that may be issued, should be closely followed by internet service providers and app operators.

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

Technology, Media & Telecommunications

Contacts

Technology, Media & Telecommunications



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

White Collar Crime



Thong Chee Kun
Partner, White Collar Crime

T +65 6232 0156

chee.kun.thong@rajahtann.com

Click [here](#) for our Partners in the Technology, Media & Telecommunications Practice.

Please feel free to also contact Knowledge 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

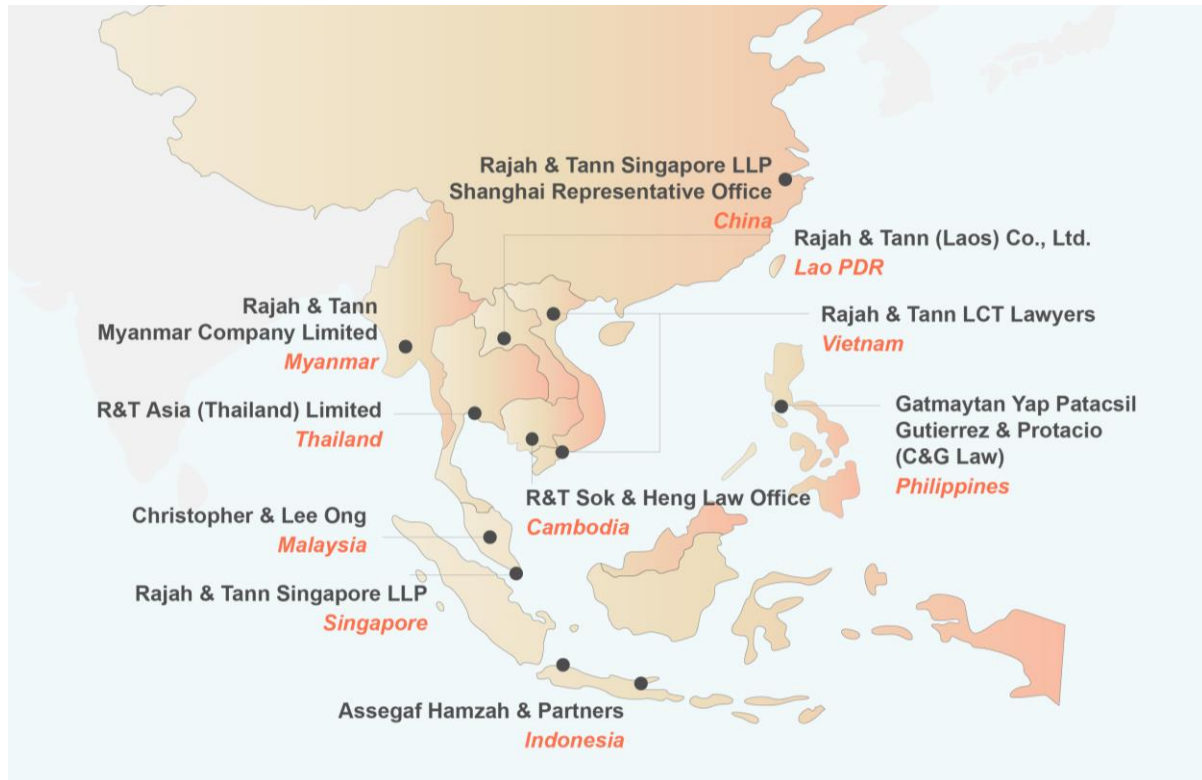
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

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.

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 Management at eOASIS@rajahtann.com.