Technology, Media & Telecommunications

The Future of Security in Digital Spaces – What New Compliance Obligations Can Online Platforms and Businesses Expect?

Introduction

With the growth of the digital economy and the increasing participation of Singaporeans in online platforms, the security of digital spaces is one of the key issues being considered by the Government. At the 2022 Committee of Supply Debates, the Ministry of Community and Information ("**MCI**") outlined its plans to build a vibrant and secure digital future.

The Minister of Communications and Information, Mrs Josephine Teo, presented a speech on 4 March 2022 as part of the MCI Committee of Supply Debates ("**Minister's Speech**"), which is available here. In her speech, the Minister set out the priorities of MCI in governing and securing Singapore's digital spaces, and gave an indication of what changes and enhancements may be expected in the digital regulatory and compliance framework.

In particular, the Minister's Speech addressed the following areas of interest:

(a) The introduction of Codes of Practice for online platforms to protect Singaporeans against harmful online content;
(b) The review of the Cybersecurity Act and update to the Cybersecurity Code of Practice to strengthen Singapore's cybersecurity; and
(c) The strengthening of data protection safeguards for consumers and businesses.

While businesses and online platforms clearly have a role to play in the security of digital spaces, the proposed plans look to introduce enforceable obligations relating to the measures that must be taken to ensure such security. In this Update, we look at the proposed changes and initiatives in the above areas and the new compliance obligations that may be expected in the near future. We also explore how these changes may affect online platforms and businesses.

Regulation of Online Content

The Minister highlighted the need to protect Singaporeans, particularly the young and vulnerable, from harmful online content.

There are currently existing measures in place, such as the Internet Code of Practice for Internet Content Providers, filtering service requirements for Internet Service Providers, and the Content Code for Over-The-Top and Video-on-Demand and Niche Services which requires parental locks to be made available for content that is rated NC16 or higher.

To further raise the baseline standard for online safety, the Minister's Speech sets out plans to introduce Codes of Practice for online platforms accessible by users in Singapore. These Codes are intended to address three new areas:

(a) **Child safety** – Platforms would be expected to have robust systems in place to minimise exposure of children and young persons to harmful content, such as content filters for child accounts or mechanisms for parental supervision.

(b) **User reporting** – User reporting has been recognised as an important way to help online platforms be aware of what content may need moderation, particularly where user-generated content may be voluminous and unwieldy to assess. Online platforms may thus be required to set up easy-to-access mechanisms for users to report harmful content. Platforms will have to be responsive in evaluating and acting on user reports, and apprise users in a timely manner of the action taken.

(c) **Platform accountability** – Platforms would be expected to provide information on what they are doing to keep users safe. This may include information on the prevalence of harmful content on their platform, the user reports they have received and acted upon, and the systems and processes they have in place to address harmful content. This will allow users to compare the approaches taken by different platforms and make informed choices of which platforms to engage.

The proposed Codes of Practice are expected to have force of law. This would place enforceable obligations on online platforms to take active steps to ensure the safety of the online environment, as set out above. It is also expected that these Codes of Practice would be updated regularly to deal with emerging issues and new technologies.

Online platforms such as social media platforms should thus map out the online safety measures which they have in place and assess them against the areas of compliance set out in the Minister's Speech so as to have a picture of the extent to which they may be compliant with such obligations and the remedial measures that may need to be taken. Platforms should be alert to any draft Codes of Practice released by MCI or any public consultations on the same, and seek to engage the relevant authorities on the practical implications or potential operational challenges of any proposed measures.

Strengthening Cybersecurity

One of the priorities of MCI is to strengthen Singapore's cybersecurity to guard against the increasing risk of cyber threats, including cyber-attacks, data breaches and ransomware. The legal framework governing cybersecurity in Singapore is currently contained in the Cybersecurity Act.

The Minister's Speech has indicated that the Cyber Security Agency of Singapore ("**CSA**") is reviewing the Cybersecurity Act and may introduce enhancements to its provisions. In this regard, the following questions are being considered:

(a) **How to raise situational awareness** – CSA must be able to look out for serious vulnerabilities so as to advise users on the necessary measures, such as patching known software vulnerabilities.

(b) **What should be considered as Critical Information Infrastructure ("CII")** – CII refer to designated computers or a computer systems located wholly or partly in Singapore, necessary for the continuous delivery of an essential service, whose loss or compromise will have a debilitating effect on the availability of the essential service in Singapore. While the Cybersecurity Act currently recognises physical networks and systems as CII, the shift to virtualisation means that it must also recognise virtual assets as CII, such as systems hosted on the cloud, so as to ensure they are properly protected.

(c) **How to secure other important digital infrastructure** – Apart from CIIs, digital infrastructure and services are also important as they form the backbone of our connectivity, computing and data storage needs. The Cybersecurity Act should thus address how to protect such infrastructure and services and facilitate quick recovery when attacked.

The review of the Cybersecurity Act is expected to be completed by 2023 and the Cybersecurity Act to be updated thereafter. Under the revised Cybersecurity Act, it is likely that these obligations will be enhanced and that new areas will be addressed, such as the security of virtual assets, although the specific requirements remain to be determined. It is nonetheless important for businesses to continually review and assess their cybersecurity standards, not just from a security standpoint, but also with a view to fulfilling compliance obligations.

CSA has also indicated in a press release of 4 March 2022 (available here) that it intends to enhance the existing Cybersecurity Code of Practice for CIIs, which sets out mandatory cyber hygiene practices. The enhancements aim to:

(a) Improve CIIs' chances of defending against cyber threat actors using sophisticated threats;
(b) Allow CIIs to be more agile to respond to emerging risks in specific domains; and
(c) Enhance coordinated defences between Government and private sectors to identify, discover and respond to cyber threats and/or attacks in a timely manner.

Examples of the proposed enhancements include:

(a) Adopting a threat-based approach to identify threat actors' common tactics and techniques used in a cyber-attack lifecycle; and
(b) Allowing the flexibility to add domain-specific practices, e.g. use of 5G technologies, on an ad-hoc basis to the relevant CII sectors and/or specific CII Owners to implement.

The enhanced Cybersecurity Code of Practice is expected to be issued to CII owners in Q2 of 2022, following briefing and consultation of key CII stakeholders.

Data Protection Safeguards

Data has been recognised as a critical resource in the digital economy. The Personal Data Protection Act ("**PDPA**") was introduced to safeguard consumers and their personal data, while also balancing the interests of businesses to harness data for innovation and growth.

In 2020, amendments to the PDPA were introduced to raise the maximum financial penalty for data breaches to S$1 million, or 10% of local annual turnover for organisations whose turnover exceeds S$10 million, whichever is higher. However, due to the economic uncertainty caused by the COVID-19 pandemic, the implementation of the new penalties was temporarily set back. The Minister's Speech has indicated that the new penalties are set to be put in force, and will take effect from **1 October 2022** so as to give sufficient lead-time to businesses.

Businesses should take note of the date from which the enhanced penalties will take effect and ensure that they are prepared to comply with their data breach obligations, including security and notification. While businesses are already subject to existing penalties for data breaches, the scale of the potential fines is set to be drastically increased.

Other Areas

The Minister's Speech has also stated the Infocomm Media Development Authority's ("**IMDA**") intention to launch an Alternative Dispute Resolution Scheme in April 2022 as a supplementary platform for consumers and small businesses if they are unable to resolve contractual disputes directly with their telco or media service providers. The scheme is intended to be affordable and effective, with service providers being mandatorily required to participate in the alternative dispute resolution process. The scheme will cover all telco and media services such as mobile services, fixed broadband services, fibre connection services and subscription TV services. The launch of the scheme follows the IMDA's public consultation in 2018. More information regarding the administration of the scheme can be found in IMDA's explanatory memo to the public consultation, which is available here.

Concluding Words

The Minister's Speech provides a preview of the changes that may be expected in the area of security and consumer safeguards in the digital space in Singapore. It helpfully sets out the areas of priority that are being considered and the regulatory tools that may be used to give effect to the proposed enhancements.

Businesses and online platforms should pay close attention to any proposed regulations and changes in legislation, including the release of any drafts and public consultations, so that they may provide their feedback, and be aware of new standards and obligations that they may have to comply with. As noted above, it is expected that some of these requirements will be constantly reviewed and updated to keep pace with emerging issues and new technologies. In this regard, we will continue to monitor the developments in this area to keep you up to date.

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

Contacts

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0751

rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0786

steve.tan@rajahtann.com

Lionel Tan
Partner, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0752

lionel.tan@rajahtann.com

Benjamin Cheong
Partner, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0738

benjamin.cheong@rajahtann.com

Tanya Tang
Partner (Chief Economic and Policy Advisor), Competition & Antitrust and Trade;
Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

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

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 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

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 | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.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

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

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

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

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.