SINGAPORE – COUNTRY REPORT

Background

This report outlines the main laws which provide law enforcement and intelligence agencies with legal powers in relation to lawful interception assistance, the disclosure of communications data, certain activities undertaken for reasons of national security or in times of emergency, and censorship of communications under Singaporean law.

1. PROVISION OF (REAL-TIME) INTERCEPTION ASSISTANCE

A broad range of government and law enforcement agencies – including, amongst others, the Singapore Police Force, the security services, government ministries, most pertinently the Ministry for Home Affairs and the Ministry of Communications and Information, and regulatory authorities such as the Info-communications Media Development Authority ("IMDA") – have the legal authority to require Telco Operators to intercept individual customer communications and to require these operators to assist them in implementing interception capabilities on the operator's network.

Strictly speaking, these authorities do not need court orders to intercept calls, emails or other communications in Singapore. The key relevant powers are found under the Criminal Procedure Code, Computer Misuse and Cybersecurity Act, Telecommunications Act and Official Secrets Act, and these powers are worded broadly. There is no general right to privacy under the Constitution of Singapore.

1.1 Telecommunications Act

Section 58 of the Telecommunications Act ("TA") gives the Minister for Communications and Information the powers to issue to the IMDA or to a Telco Operator such directions as the Minister thinks necessary. This may include:

- the prohibition and regulation of telecommunications as necessary;
- taking control of the use of any telecommunication system and equipment; and
- the stopping, delaying, and censoring of messages as the Minister thinks necessary.

The financial penalties for non-compliance include a fine of up to the higher of:

- 10% of the annual turnover of the part of the business granted the licence; or
- SG$1 million; and
- if the telecommunications operator continues to not comply a further fine of up to SG$100,000 for every continuing day of non-compliance may also be imposed.

These powers can remain confidential if the Minister is of the opinion that the disclosure of such directions is against public interest.

Whilst the appeal processes envisioned under the TA do not apply to the exercise of the Minister's discretion under section 58, a Telco Operator could seek judicial review of such a decision by the Minister if they can demonstrate that there was illegality, irrationality or procedural impropriety in the exercise of the Minister's decision.

1.2 The Criminal Procedure Code

Under Part IV of the Criminal Procedure Code ("the CPC"), authorities are given broad powers to intercept communications. Section 39 of the CPC permits police officers or "authorised persons", as appointed, to access, inspect and check the operation of a computer that they have reasonable cause to suspect have been used in connection with an arrestable offence or (more broadly) the police officer can use any such computer to search for any data available or contained within. "Authorised persons", for the purposes of section 39 of the CPC, are forensic specialists as appointed under section 65A of the Police Force Act or any other person, authorised in writing by the Commissioner of Police.

Computer is defined broadly in the Computer Misuse and Cybersecurity Act ("CMCA") (a definition which also applies

under the CPC). This would include any data processing facility e.g. a smartphone.

The exercise of powers under section 39 of the CPC are not subject to judicial approval. It is also worth noting that section 18(2) (of the CPC) provides that the exercise of a police officer of these powers may not be called into question on the ground the officer lacked authority to investigate.

Section 40 of the CPC further grants powers to the Public Prosecutor who may authorise a police officer or "authorised person" to access and/or decrypt any data which is necessary for investigating the arrestable offence. This includes data stored on "computers" accessed under section 39 of the CPC.

The legislation is broadly worded and, in theory, allows both overt as well as covert examination. The extent to which these powers are used covertly in practice is not information that is in the public domain. However, these powers could technically be used to listen to individuals' phone calls without their knowledge in real-time.

Obstructing access or failing to comply with a requirement of a police officer or forensic specialist, under the provisions of section 39 of the CPC can result in a fine of up to SG$5,000 or imprisonment for a term not exceeding 6 months or both.

Obstructing access to the data or failing to provide technical or other assistance with decryption, for failing to comply with the provisions of section 40 of the CPC can result in a fine of up to SG$10,000 or imprisonment of up to 3 years or both. If the crime is of a higher threshold, e.g. terrorism, kidnapping, murder etc. then the punishments can be a fine of up to SG$50,000, imprisonment of up to 10 years or both.

1.3 Computer Misuse and Cybersecurity Act

Under section 15A of the CMCA, where the Minister of Home Affairs is satisfied that it is necessary for the purposes of preventing, detecting or countering any threat to national security, essential services or defence of Singapore or foreign relations of Singapore, in order to prevent, detect or counter any threat to a computer or computer service or any class of computers or computer services they may:

- direct a police officer or authority to exercise their powers under section 39 or 40 of the CPC (s.15A(2)(a)) (i.e. allowing access to data stored on any computer);
- order a police officer, prosecutor or other authority to direct a person to provide any information necessary to identify, direct or counter any threat to a computer or computer service (s.15A(2)(b));
- order any person to provide to the Minister of Home Affairs or any public officer any information (including real-time information) obtained from any computer controlled or operated by that person or obtained from another person that is necessary to identify, detect or counter any such threat to a computer or computer service (s. 15A(2)(c)) [emphasis added]; and
- order a report of a breach or an attempted breach of security to be provided relating to any computer controlled or operated by the specified person (s. 15A(2)(d)).

Again, this could, for example, be used to listen to individuals' phone calls without their knowledge in real-time. However given that this would be conducted covertly by the Singapore government, there is little publicly available information on the exercise of such powers in practice.

Punishments for failing to comply with any request under section 15A CMCA can result in fines of up to SG$50,000 or to imprisonment for a term not exceeding 10 years or both.

The powers under the CMCA are broadly drafted and are supported by section 14 of CMCA which states nothing in the CMCA shall prohibit a police officer, an authorised person within section 39 of the CPC or any other duly authorised law enforcement officer from lawfully conducting investigations pursuant to the powers conferred on them under any written law. Section 16 of the CMCA further provides that any police officer may arrest without warrant any person reasonably suspected of committing an offence under the CMCA.

2. DISCLOSURE AND RETENTION OF COMMUNICATIONS DATA

2.1 Telecommunications Act

Section 59 of the TA states that the IMDA may order any person to produce any document or information for the purposes of an investigation. This would include the content of messages and the metadata surrounding it.

Powers of production are replicated in the Telecom Competition Code ("TCC"). At 11.6 of the TCC telecom operators, as well as certain other businesses operating in the telecommunications sector, may be required to produce specified documents or information as determined by the IMDA. Under this provision, the IMDA is also entitled to physically inspect accounts, documents, records, facilities and operations.

The penalties of non-compliance under the TCC are set out at 11.4.4 and broadly track those discussed above under section 58 of the TA – i.e. fines of up to 10% of global turnover or SG$1 million. In addition, under 11.4.5 of the TCC, the IMDA has the power to revoke telecommunications licences in serious cases of breach.

Any Telco Operator aggrieved by any decision or direction of the IMDA (either under the TA or in a Code of Practice) may within 14 days of the receipt of the decision or direction request that the IMDA reconsider the matter or appeal to the Minister. These powers of appeal are derived from section 69 of the TA. The reconsideration request power cannot be exercised to both the IMDA and the Minister; only one can be consulted. If both are consulted at the same time, the appeal is withdrawn.

The IMDA has the power to confirm, vary or reverse any decision or direction. If the Telco Operator is aggrieved by the decision of the IMDA, the Telco Operator can further appeal

to the Minister within 14 days of the receipt of that decision. Alternatively an appeal can be filed directly with the Minister. If an appeal is filed with a Minister, there is no recourse to the IMDA. In either case, such an appeal must state as concisely as possible the circumstances for the appeal, the issues and ground for this appeal and submit all relevant facts, evidence and arguments for the appeal. If these requirements are not complied with, the appeal can be rejected.

The Minister's decision is final under the TA, and until there is a final decision, the decision or direction that is being appealed must be complied with. Therefore, in practice, any interception or control, stopping, delaying or censoring would need to be complied with until the final decision of the Minister, who in turn may have given the direction that is being appealed. An aggrieved party who has unsuccessfully appealed to the Minister does have one final challenge by initiating a judicial review in the courts.

2.2 The Personal Data Protection Act

(a) Collection, Use and Disclosure of Data

The Personal Data Protection Act ("PDPA") sets out various restrictions surrounding the collection, use, disclosure and care of personal data. Personal data is defined in the PDPA as data, whether true or not, about an individual who can be identified a) from that data; or b) from that data and other information to which the organisation has or is likely to have access. The PDPA is regulated by the Personal Data Protection Commission ("PDPC").

However, section 4(1)(c) of the PDPA states the restrictions on use, collection and disclosure of personal data does not impose any obligation on a public agency or organisation if acting as such. This would include the government, its ministries or state, tribunal or statutory bodies.

Furthermore, the collection, use or disclosure of personal data without consent is permitted if necessary in the national interest or for any investigation or proceedings, (and if in relation to collection, such collection without consent is limited to if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data). These appear as some of the exceptions under the Second, Third and Fourth Schedules of the PDPA. Under the Fourth Schedule of the PDPA, disclosure without consent of an individual is also permitted if, requested in writing as, necessary for the functions of an officer of a law enforcement agency. As such, the provisions of the PDPA cannot generally be relied on to avoid obligations to disclose personal data to government authorities.

(b) Retention of Data

Telco Operators who hold a Service Based Operator ("SBO") or Facility Based Operator ("FBO") licenses regulated by the IMDA and who provide certain services are required – under the applicable license conditions – to keep a register of their subscriber details including their name, address, date of birth and nationality. In the case of FBO License holders this covers subscribers of IP telephony services; as far as SBO license holders are concerned the relevant services include IP telephony services, satellite mobile telephone and data services, mobile virtual network operations, and voice and data services which mask call line identity. In either case the relevant license holder will also be required to keep subscribers' call detail records for a period of at least 12 months.

The PDPA also sets out a retention obligation which states when an organisation has to cease to retain personal data of individuals or remove the means by which the personal data can be associated with particular individuals (section 25 PDPA). This must occur as soon as it reasonably practical after the purpose for collecting that data has become obsolete.

As each organisation is different, the PDPA does not specify a fixed duration of time for which an organisation can legitimately retain personal data. The PDPC explain, in their Advisory Guidelines on Key Concepts in the PDPA ("the PDPA Guidelines") that whilst the PDPA does not prescribe a specific retention period for personal data, organisations would need to comply with any legal or specific industry-standard requirements. The length of the retention of data, including communication data as it relates to personal data, would be determined when considering:

- the purpose for which the personal data was collected; and
- the legal or business purposes for retaining personal data. This may include situations as set out in the PDPA Guidelines where:
  - The personal data is required for an on-going legal action involving the organisation;
  - Retention of personal data is necessary in order to comply with the organisation's obligations under applicable laws and regulations; or
  - The personal data is required for the organisation to carry out its business operations such as generating annual reports or performance forecasts.

Under section 50(4) of the PDPA, an organisation is required to retain records of an investigation for one year after the conclusion of the investigation or any longer period specified in writing by the PDPC. Further investigatory powers of the PDPC are discussed in the Ninth Schedule of the PDPA. On retention, there is a time limit to the PDPC's retention of any documents obtained under warrant. Section 3(12) of the Ninth Schedule only allows the retention of any document, by the PDPC or its inspectors, for a period of not more than 3 months.

In addition to legislation, the common law, for instance the law of breach of confidence can offer indirect remedies for privacy breaches.

3. NATIONAL SECURITY AND EMERGENCY POWERS

Law enforcement agencies in Singapore can and do request information from persons or organisations that will help in investigations into criminal cases. As discussed above, the TA goes further and allows control over telecommunication networks.

Section 72 of the Organised Crime Act 2015 makes reference to the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act. These two acts confer production and search order powers on prosecutors and the police to apply to court in order to gather information in relation to criminal conduct.

3.1 Powers of Intelligence Services

The two key security services: The Security and Intelligence Division ("SID") and the Internal Security Division ("ISD") have a broad scope of powers.

The SID is a separate branch from the Ministry of Defence and is highly clandestine. Responsible for international security with a wide geographical remit, in contrast to the ISD, its actions, powers and personnel are rarely revealed. Little is known about their policies and procedures and how they gather intelligence.

The ISD is an offshoot of the Ministry of Home Affairs and is concerned with domestic Singaporean affairs. The ISD is regulated by a number of acts including the Internal Security Act (the "ISA"), the CPC, the Official Secrets Act (discussed in detail below, the "OSA") and the Maintenance of Religious Harmony Act. Under the ISA, in section 8B(2) there shall be no judicial review in any court of any act done or decision made by the President or the relevant Minister for any action under the ISA except with regard to procedural requirements. However, section 13 of the ISA states that any power to order detention (under section 8) or suspend that detention (under section 10) affords an advisory board review powers at periods no longer than 12 months.

3.2 Telecommunications Act

As referred to above, if it appears to the Minister for Communications and Information to be requisite or expedient to do so:

(a) on the occurrence of any public emergency, in the public interest or in the interests of public security, national defence, or relations with the government of another country; or

(b) to discharge or facilitate the discharge of an obligation binding on the Government by virtue of its being a member of an international organisation or a party to an international agreement;

(c) to attain or facilitate the attainment of any other object the attainment of which is in the opinion of the Minister requisite or expedient in view of the Government being a member of an international organisation or a party to an international agreement; or

(d) to enable the Government to become a member of an international organisation or a party to an international agreement,

the Minister may, after consultation with the IMDA or any telecommunication licensee, give such directions to the IMDA or that licensee as are necessary in the circumstances of the case. This may include:

(a) provisions for the prohibition or regulation of such use of telecommunications in all cases or of such cases as may be considered necessary;

(b) provisions for the taking of, the control of or the usage for official purposes of, all or any such telecommunication system and equipment; and

(c) provisions for the stopping, delaying and censoring of messages and the carrying out of any other purposes which the Minister thinks necessary.

The IMDA and any telecommunication licensee must give effect to any such direction given to them or they will commit an offence as set out above.

If the Minister notifies the subject of such a direction that the disclosure of the direction is against the public interest then it must be kept confidential.

The Minister may pay compensation for any damage caused to a telecommunication licensee by reason of its compliance with such directions. If any doubt arises as to the existence of a public emergency or as to whether any act done under this section was in the public interest or in the interests of public security, national defence or relations with the government of another country, a certificate signed by the Minister is considered conclusive evidence of the matters stated therein.

3.3 Official Secrets Act

The OSA is Singapore's primary legislation protecting state secrets and official government information mainly related to national security. Amongst other things, it prohibits, under section 5 the disclosure of such information by those holding it whether in their official capacity or otherwise.

Section 9 of the OSA allows the Minister of Home Affairs, if it considers it expedient in the public interest, to order any person who owns or controls any telecommunication system in Singapore (including private networks), to produce the originals / transcripts of any messages sent from/to any place in Singapore, by any telecommunication system means. Moreover, under Section 10, police officers of the rank of sergeant or higher or certain members of the armed forces may require any person to provide any information in their possession relating to a potential offence under this act. This could include the content/metadata of customers'

communications in the possession of Telco Operators.

Where a Justice of the Peace in Singapore considers that an offence under the OSA may have occurred, they may issue a search warrant under Section 15 of the OSA allowing a police officer to search any premises covered by the warrant. However, Section 15(5) incorporates a wide carve-out which allows police officers of the rank of sergeant or above to execute search orders without judicial approval in cases of emergency.

4. CENSORSHIP

The Singapore government takes the view that censorship of political, racial, religious issues is necessary to avoid upsetting Singapore's society. Censorship occurs on television, in films, in print media, music, video games and the arts. A government agency can control customer communications under the TA and the IMDA is the main government body tasked with regulating these entities (together with other regulatory agencies).

There is no specific content censorship for telecommunications over phone calls or texts (which are not published) but the Minister of Communications and Information can give the IMDA directions to censor messages on the network under section 58(3) of TA.

4.1 Internet Code of Practice, IMDA and Broadcasting (Class Licence) Notification

Material that is broadcast, such as television programs or content published on the internet (including social media) is governed by codes of practice issued by the IMDA. The Internet Code of Practice ("ICOP"), under section 2, requires that licensees (i.e. Internet Content Providers and Internet Service Providers) use their best efforts to ensure that prohibited material is not broadcast via the internet to users in Singapore. Prohibited material is defined in section 4 of ICOP and is material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws.

Under the Broadcasting Act, the IMDA has the power to impose sanctions, including fines, on licensees who contravene ICOP. Internet Content Providers also need to remain mindful of the Class Licence Conditions which are set out in the Schedule to the Broadcasting (Class Licence) Notification. These conditions set out further guidelines for Internet Content Providers to adhere to which include: pre-registration if the Internet Content Providers is engaged in the propagation, promotion or discussion of political or religious issues; assisting IMDA with any information requests or investigations and ensuring the service is not for furtherance of games and lotteries; horse-racing gambling; prostitution; professional advice given by persons without Singapore-recognised qualifications, broadcasting of films or sounds not approved by the Films Act or IMDA.

ICOP and the class conditions are unlikely to apply to telephone communications but do apply to broadcast media which includes internet access (networks) and content providers.

4.2 Blocked websites

The Singapore government through the IMDA maintains a list of blocked websites. The IMDA, under acts such as the Remote Gambling Act and Undesirable Publications Act also bans websites labelled under categories like pornography, cults, violent crime, criminal skills and gambling. Under the Remote Gambling Act, it is an offence punishable by imprisonment and fines to place bets on overseas gambling websites from Singapore.

Under the Class Licence Conditions, if the IMDA is satisfied that content on a website is undesirable, harmful or obscene, the IMDA will give Internet Service Providers written notice that users should be prevented from accessing that content. The Internet Service Provider will then be required to take all reasonable steps prevent such end-users from accessing that content.

4.3 Sedition Act

Under Sections 3 and 4 of the Sedition Act, any person who in respect of any act, speech, word, publication or thing which is seditious, that being a tendency to bring hatred or contempt feelings against the government; excite Singaporean citizens/residents against any law; bring any hatred or contempt against the administration of justice in Singapore; raise discontent or disaffection against citizens or residents of Singapore or promote feelings of ill-will or hostility to different races or classes of Singapore will be guilty to a fine of SG$5,000 on a first offence or imprisonment of 3 years though this can increase to five years if a subsequent offence.

This too will likely not apply to personal, non-inciteful telephone calls, but the section 4 (1)(b) includes the act to "utter any seditious words" and given the broad investigatory powers of the Singapore state this is worth noting.

4.4 Films Act

Under the Films Act, content that is currently banned includes film content which is against national interests or corrosive to society.

4.5 Electronic Transactions Act

The Electronic Transactions Act ("ETA") implements the United Nations Convention on the Use of Electronic Communications in International Contracts in Singapore. Section 26(1) of the ETA specifically provides that network service providers ("NSPs") will not attract criminal or civil liability for third party materials for the mere reason that they are the host, subject to the NSP's obligations under other regulatory regimes. NSP is not defined under the ETA. However, since the ETA makes reference to a NSP's liability under the Copyright Act, the definition of NSP under the Copyright (Network Service Provider) Regulations is likely to apply, i.e. a NSP means "a person who (a) provides services, relating to, or provides connections for, the transmission or routing of data; or (b) provides, or operates facilities for, online services or network access."

5. OVERSIGHT OF THE USE OF POWERS

Other than as discussed in the relevant sections above and below, there is generally little independent oversight of the broad powers granted to government agencies in Singapore. Singapore administrative law does however provide for a judicial review mechanism which allows for the review by the courts of executive actions that are alleged to be ultra vires (outside the scope of the powers of the relevant executive body).

6. PUBLICATION OF AGGREGATE DATA RELATING TO USE OF GOVERNMENT POWERS

There are no overarching restrictions on the publication by Telco Operators of anonymised aggregate data in Singapore.

The Singapore Government does not publish aggregate data relating to its use of the powers described in this report.

7. CYBERCRIME

7.1 Computer Misuse and Cybersecurity Act

Under the CMCA, "computer" has a broad definition and therefore the legislation also has relevance for smartphone/telecommunication providers. There are a number of offences:

(a) Unauthorised access to computer material (section 3)

Any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence. Access for the purposes of the offence includes altering or erasing data or the program; copying or moving it; using it; or causing it to be output from the computer (whether by being displayed or otherwise). For a first-time conviction the penalties for such an offence are a fine of up to SG$5,000 or imprisonment for up to 2 years or both. If it is a second or subsequent conviction, the accused can be liable to a fine of up to SG$10,000 or imprisonment for up to 3 years or both. If damage is caused then a person convicted of the offence shall be liable to a fine not exceeding SG$50,000 or to imprisonment for a term not exceeding 7 years or both. The act can attract liability regardless of whether or not it is directed at any particular program or data.

(b) Access with intent to commit or facilitate commission of offence (section 4)

A person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years shall be guilty of an offence. Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding SG$50,000 or to imprisonment for a term not exceeding 10 years or both.

(c) Unauthorised modification of computer material (section 5)

Any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence. The act can attract liability regardless of whether or not it is directed at any particular program or data.

(d) Unauthorised use or interception of computer service (section 6)

Any person who knowingly:

- secures access, without authority, to any computer for the purpose of obtaining, directly or indirectly, any computer service;
- intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of any device; or
- uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing either of the two previous offences

shall be guilty of an offence. It is irrelevant if the act is not directed at any particular program or data, the act can still attract liability.

(e) Unauthorised obstruction of use of computer (section 7)

Any person who knowingly or without authority or lawful excuse interferes with or interrupts or obstructs the lawful use of a computer or impedes or prevents access to or impairs the usefulness or effectiveness of any program or data stored in a computer shall be guilty of an offence.

The penalties for offences under sections 5, 6 and 7 are, on first conviction, a fine of up to SG$10,000 or imprisonment for up to 3 years or both. For subsequent convictions, the accused will be liable for a fine up to SG$20,000 or imprisonment for up to 5 years or both. If any damage is caused, a person convicted of the offence shall be liable to a fine not exceeding SG$50,000 or imprisonment for a term not exceeding 7 years or both.

(f) Unauthorised disclosure of access code (section 8)

Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if they did so for any wrongful gain; any unlawful purpose; or knowing that it is likely to cause wrongful loss to any person.

Offenders are liable on first conviction to a fine of up to SG$10,000 or imprisonment for up to 3 years or both. For subsequent convictions, the accused will be liable for a fine up to SG$20,000 or imprisonment for up to 5 years or both.

(g) Supplying etc. personal information obtained in contravention of certain provisions (section 8A)

This provision was part of 2017 amendments to the CMCA. A person is guilty of an offence if the person, knowing that personal information about another individual was obtained by an act done in contravention of sections 3, 4, 5 or 6, retains or obtains that personal information or supplies (or offers to do so) that personal information. If obtained but not for the purposes of an offence this can be used as a defence to this crime. This is designed, as exemplars in the legislation describe, to criminalise credit card and personal information transmission and distinguish between illegal transfer/use of that data and legitimate uses to flag this personal information e.g. for the purposes of an investigation.

Offenders are liable on first conviction to a fine of up to SG$10,000 or imprisonment for up to 3 years or both. For subsequent convictions, the accused will be liable for a fine up to SG$20,000 or imprisonment for up to 5 years or both.

(h) Obtaining etc. items for use in certain offences (section 8B)

Also part of the 2017 amendments, a person is guilty of an offence if the person obtains or retains any item (which includes any device, including computer programs or passwords, access codes or similar data) for the purposes of committing or facilitating, or supplying to facilitate or commit, offences under sections 3, 4, 5, 6 or 7.

Offenders are liable on first conviction to a fine of up to SG$10,000 or imprisonment for up to 3 years or both. For subsequent convictions, the accused will be liable for a fine up to SG$20,000 or imprisonment for up to 5 years or both.

(i) Enhanced offence for protected computers (section 9)

If access is obtained to protected computers which are computers or programs or data used for:

(i) the security, defence, or international relations of Singapore;

(ii) the existence or identity of a confidential source of information relating to criminal law enforcement;

(iii) the provision of services for communications, banking and financial services, public utilities, public transportation or public key infrastructure; or

(iv) the provision of public safety and emergency services such as the police, civil defence and medical services

then a person who commits offences under sections 3, 5, 6 or 7 shall receive an enhanced punishment which will be a fine not exceeding SG$100,000 or imprisonment for a term not exceeding 20 years or both.

(j) Overseas offences (section 11)

The final notable amendment of the CMCA in the 2017 revisions was the extension of criminal liability to any person, whatever his nationality or citizenship, outside as well as within Singapore. This applies if the accused was in Singapore at the material time; the computer, program or data was in Singapore or there is significant risk of serious harm in Singapore.

Serious harm in Singapore is defined to include: "illness, injury, or death of individuals in Singapore; disruption of any essential service in Singapore; disruption of public confidence in the government or state organ or damage to the national security, defence or foreign relations of Singapore." Examples of diminishment to public service included in the legislation include publication to the public of medical records of patients in a Singaporean hospital or provision to the public of the access of bank account numbers of a Singaporean bank. Examples of diminishment of public confidence in a state organ include public access to confidential documents belonging to a ministry of government.

Two additional points which are noteworthy are that under the CMCA, any police officer may arrest without warrant any person reasonably suspected of committing an offence under this act (section 16). For two or more acts to be amalgamated together, they must be the same type of offence, involving the same computer within the same 12 months (section 11A).

The courts have jurisdiction to hear and determine all offences under the CMCA, under section 12 of the CMCA, with the power to impose the full penalty or punishment in respect of any offence under this act. However, the police and ministerial powers can avoid judicial discretion (for example, section 15A discussed below) and section 12 of the CMCA is subject to anything contrary in the CPC (i.e. section 39 of the CPC which allows police officers to intercept communications without judicial oversight).

8. CYBERSECURITY

8.1 The CMCA currently focuses on cybercrime.

The Singaporean government is in the process of introducing legislation specifically focused on cybersecurity.

8.2 Cybersecurity under the CMCA (section 15A)

As discussed above, section 15A CMCA states that if the Minister of Home Affairs is satisfied that it is necessary for preventing, detecting or countering any threat to national security, essential services or the defence of Singapore or foreign relations, the Minister, using a certificate under his own hand, can order such measures to comply with requirements to prevent, detect or counter any threat to a computer or a computer service, which can include power to access a computer and decrypt information (as under sections 39 and 40 of the CPC).

8.3 Telecommunication Cybersecurity Code of Practice

The IMDA has formulated codes of practice to enhance the cyber security preparedness for designated licensees. The codes are currently imposed on major Internet Service Providers in Singapore for mandatory compliance, and their coverage includes their network infrastructure providing Internet services. As well as security incident management requirements, the codes include requirements to prevent, protect, detect and respond to cyber security threats. This cybersecurity code of practice was formulated using international standards and best practices including the ISO / IEC 27011 and IETF Best Current Practices.

This is assisted by the IMDA and the Info-communications Singapore Computer Emergency Response Team (ISG-CERT) which is a dedicated cyber-security and threat response service for the telecoms and media sector. These are subject to change with the new Cybersecurity Bill discussed below.

8.4 Draft Cybersecurity bill

In addition to the existing legislation outlined above, a new Cybersecurity Bill is currently under review by the Ministry of Communications and Information and the Cyber Security Agency ("CSA") of Singapore. This is an overarching, sector-agnostic piece of legislation, which, if passed, will complement, and in some cases supersede, existing legislation that pertains to cybersecurity or the sharing of confidential information, e.g. banking and privacy rules. Parliament in Singapore intends to introduce this as legislation in 2018.

The Draft Bill does contains various proposals worth highlighting such as the introduction of cyber-attack incident reporting obligations, the licensing of cyber-security practitioners (although under current proposals this will not apply to in-house cyber security specialists) and regulatory requirements for critical information infrastructure ("CII") owners (which will include computer systems that are necessary for the continuous delivery of "essential services" – which currently includes the Banking and Finance, Energy, Government, Infocomm, Aviation, Healthcare, Land Transport, Maritime, Media, Security & Emergency and Water sectors).

The Bill will give the CSA powers to order investigations into suspected cyber-attacks, and information must be surrendered or can lead to fine or jail term, superseding existing but limited privacy rules.

CII owners will be given a grace period to implement measures to comply with the Bill but unless contractual obligations are put in place on vendors they are ultimately responsible for the cybersecurity of their CIIs. CIIs will be required to establish reasonable mechanisms and processes to detect cybersecurity threats and incidents, with further guidance from the CSA to follow. The powers of the Cybersecurity Commissioner will be broad including seizure, requests for information and assistance with investigations.

Law stated as at 20 November 2017.