MALAYSIA – 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 Malaysian law..

1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

Legislation which specifically provides authority to intercept communications is summarised below. Where not explicit, these rights can be interpreted widely to require network operators and service providers to assist law enforcement and intelligence agencies in their surveillance and censorship activities.

1.1 Criminal Procedure Code (the "CPC")

Under section 116B, a police officer conducting a search under the CPC is to be given access to computerized data whether stored in a computer or otherwise. For the purpose of this section, "access" includes being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of the computerized data.

Section 116C gives the law enforcement agencies very wide powers to intercept communications which may be evidence related to an offence.

Under section 116C, the Public Prosecutor (the Attorney General, the Solicitor General in certain circumstances or the Deputy Public Prosecutor as may be appointed by the Public Prosecutor) may authorise a police officer to intercept any message transmitted or received by any communication, which may be evidence related to the commission of an offence. The CPC defines "offence" as any act or omission made punishable by any law for the time being in force, including offences such as money laundering or gambling. The Public Prosecutor may also require a communications service provider to intercept and retain a specified communication or communications of a specified description received or transmitted, or about to be received or transmitted by that communications service provider, or authorise a police officer to enter any premises and to install on such premises any device for the interception and retention of a specified communication or communications of a specified description and to remove and retain such device.

Section 116C is silent as to whether a warrant is required, which will ultimately depend on the offence under investigation and the circumstances at hand. Under sections 62 and 116A, a search without warrant is possible if there is reasonable cause for suspecting that there is evidence of a security offence or concealed organised crime or any stolen property is concealed in any place and there are good grounds to believe that a delayed search is likely to result in their removal. A "security offence" has the same meaning as under the Security Offences (Special Measures) Act 2012 (set out immediately below).

1.2 Security Offences (Special Measures) Act 2012 (the "SOSM")

Section 6 SOSM allows the Public Prosecutor (the Attorney General) and police officers to intercept all communications likely to contain any information relating to the commission of a security offence. A "security offence" is an offence stated in chapter VI (offences against the state) or chapter VIA (offences relating to terrorism) of the Penal Code. For example, activity detrimental to parliamentary democracy, sabotage, waging war against the Yang di-Pertuan Agong (the King of Malaysia) and committing terrorist acts.

Section 6(1) states that the Public Prosecutor may authorise any police officer or any other person to:

(a) intercept, detain and open any postal article in the course of transmission by post;

(b) intercept any message transmitted or received by any communication; or

(c) intercept or listen to any conversation by any communication,

if he considers that it is likely to contain any information relating to the commission of a security offence.

For the purposes of section 6, the term 'communication' means "a communication received or transmitted by post or a telegraphic, telephonic or other communication received or transmitted by electricity, magnetism or other means". This gives the police the power to intercept a wide range of communications, including electronic communications.

Under section 6(2) SOSM, a police officer not below the rank of Superintendent of Police may do any of the above without authorisation of the Public Prosecutor in urgent and sudden cases where immediate action is required leaving no time for deliberation. In practice, this may give police the power to intercept communications in a wide range of circumstances, including electronic communications.

1.3 Communications and Multimedia Act 1998 (the "CMA")

There are a wide range of offences provided for under the CMA, including breach of licence conditions and telecommunication-specific issues such as improper or fraudulent use of network facilities/services.

Section 252 CMA allows an authorised officer or a police officer of or above the rank of Superintendent to intercept or to listen to any communication if a public prosecutor considers a communication is likely to contain information relevant to an investigation into an offence under the CMA or its subsidiary legislation.

The CMA defines "authorised officer" as any public officer or officer appointed by the MCMC and authorised in writing by the Minister with responsibility for communication and multimedia (presently the Minister of Communications and Multimedia (the "Minister")). "Intercept" is defined as the aural or other acquisition of the contents of any communications through the use of any electronic, mechanical, or other equipment, device or apparatus. "Communications" is defined as any communication, whether between persons, objects, or persons and objects, in the form of sound, data, text, visual images, signals or any other form or any combination of those forms.

Furthermore, section 265 CMA gives the Minister the right to require implementation of authorised interception capabilities by a licensee or class of licensees. A "licensee" is a person who either holds an individual licence or undertakes activities which are subject to a class licence. There are four categories of license that govern the relevant licensable activities: Network Facilities Service Provider; Network Service Providers; Applications Service Provider; and Content Applications Service Provider. A telecommunications service provider must be licensed if it is providing licensable activities.

Please note that section 265 is silent as to whether the implementation of the authorised interception capability would only be for purposes pursuant to a CMA offence. As a result, if it were to be read widely, it may cover offences outside of the CMA.

Section 38 gives the Minister the power to suspend or cancel an individual licence by declaration in certain circumstances, for example, if the licensee has failed to comply with the CMA or the conditions of its individual licence or the suspension or cancellation is in the public interest. Section 48 also provides similar cancellation powers to the Minister in respect of a class licensee.

Section 254 gives an authorised officer additional powers for the purposes of the execution of the CMA or its subsidiary legislation for specified purposes, including:

(a) to require the production of records, accounts, computerised data and documents kept by a licensee or other person and to inspect, examine and to download from them, make copies of them or take extracts from them; and

(b) to make such inquiry as may be necessary to ascertain whether the CMA and its subsidiary legislation have been complied with.

1.4 Copyright Act 1987 (the "Copyright Act")

Offences under the Copyright Act include: making for sale or hiring any infringing copy, distributing infringing copies, and circumvention of technological protection measures.

Under section 50B of the Copyright Act, the Public Prosecutor (the Attorney General) may authorise an Assistant Controller or a police officer not below the rank of Inspector Officer to intercept or to listen to any communications for the purpose of any investigation into an offence under the Copyright Act or its subsidiary legislation if he considers that the communication is likely to contain information relevant to the investigation.

An Assistant Controller comes under the purview of the Intellectual Property Corporation of Malaysia (the "MYIPO"), and is appointed or deemed to be appointed by the Director General of the MYIPO under section 5 Copyright Act.

Section 43H Copyright Act provides a copyright owner whose right has been infringed to notify (in the manner determined by the Minister charged with the responsibility for intellectual property at the relevant time) a service provider to remove or disable access to the electronic copy on the service provider's network within 48 hours of receipt of notification, although it is possible for a counter-notification to be issued by the person whose electronic copy of the work was removed or to which access has been disabled to require the service provider to restore the electronic copy or access to it within 10 business days, subject to further notification from the copyright owner.

1.5 Malaysian Anti-Corruption Commission Act 2009 (the "MACC")

Under section 43 MACC, if the Public Prosecutor (the Attorney

General) or an officer of the Malaysian Anti-Corruption Commission (the "Commission") of the rank of Commissioner or above, as authorised by the Public Prosecutor, considers that it is likely to contain any information which is relevant for the purpose of an investigation into an offence under the MACC, it may authorise any officer of the Commission to intercept any message transmitted or received by any telecommunication, or to intercept, listen to and record any conversation by any telecommunication, and listen to the recording of the intercepted conversation.

Section 47 also imposes a legal obligation on every person to give information if required by an officer of the Commission or a police officer on any subject which it is such officer's duty to inquire into under the MACC and which is in that person's power to give.

1.6 Certain interception powers are also authorised to particular law enforcement and intelligence agencies under the Kidnapping Act 1961, the Strategic Trade Act 2010, the Dangerous Drugs Act 1952, and the Dangerous Drugs (Forfeiture of Property) Act 1988.

2. DISCLOSURE OF COMMUNICATIONS DATA

As established above, various statutes provide wide powers of access, information gathering, search and seizure to law enforcement and intelligence agencies, which do not specifically distinguish between metadata and other types of data relating to communications, but may entail disclosure of such information. The following statutes give the relevant authorities wide powers of search and seizure that may include the right to access communications stored on a computer server. However, this is not an exhaustive list of the access rights given to law enforcement officers under Malaysian law. Many other statutory sources grant rights of search and seizure where there has been a breach of the relevant legislation, and information access rights given to law enforcement authorities are generally in relation to a commission or suspected commission of a crime or contravention of particular laws. Depending on the circumstances surrounding the request (i.e. if there is an offence being investigated), access rights may be wide, including entering premises by force and access to any data (including computerized data) as well as a right to intercept communications. Industry-specific regulators may also have inspection and audit requirements.

2.1 Computer Crimes Act 1997 (the "CCA")

The CCA generally protects against the misuse of computers, for example, hacking (see below for further information on the offences). The CCA also provides wide powers of search, seizure and arrest to a police officer of or above the rank of Inspector. Under section 10, whenever there is reasonable cause to believe that in any premises there is evidence of the commission of an offence under the CCA, an officer may be empowered to enter the premises, by force if necessary, and there to search for, seize and detain any such evidence and he shall be entitled to:

(a) have access to any program or data held in any computer, or have access to, inspect or check the operation of, any computer and any associated apparatus or material which he has reasonable cause to suspect is or has been in use in connection with any offence under the CCA;

(b) require (i) the person by whom or on whose behalf the police officer has reasonable cause to suspect the computer is or has been so used; or (ii) any person having charge of or otherwise concerned with the operation of, the computer, apparatus or material, to provide him with such reasonable assistance as he may require; and

(c) require any information contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible.

Section 10(3) of the CCA also states that any police officer may arrest without a warrant any person whom he reasonably believes to have committed or to be committing an offence against the Act. Section 11 of the CCA makes it an offence to obstruct a search when a police officer or authorised officer is executing any duty imposed or conferred by law. If there is a court order or search warrant, the network operators and service providers may be liable for contempt of court if they refuse to assist.

2.2 Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (the "AMLA")

Section 31 AMLA confers wide powers on an investigating officer to conduct a search without a warrant if the officer is satisfied or has reason to suspect that a person has committed an offence under AMLA. These powers include searching for any property, record, report or document, and inspecting and taking possession of or making copies of or taking extracts from any record, report or document so seized and detained, and detaining them for such period as he deems necessary.

Section 37 requires any person to deliver any property, document or information which an investigating officer has reason to suspect:

(a) has been used in the commission of an offence under AMLA: or

(b) is able to assist in the investigation of an offence under AMLA

that is in the possession or custody of, or under the control of, that person or is within the power of that person to furnish.

Under section 67(1), similar powers exist where the competent authority or an enforcement agency has reason to believe that a person is committing, has committed or is about to commit an offence under AMLA.

The definition of "document" for these purposes is very wide

and may be interpreted to include metadata relating to electronic communications.

2.3 Anti-Trafficking In Persons Act and Anti-Smuggling of Migrants Act 2007 (the "ATPAASMA")

Section 32 ATPAASMA stipulates that any enforcement officer conducting a search under ATPAASMA shall be given access to computerized data, whether stored in a computer or otherwise. For this purpose, the enforcement officer shall be provided with the necessary password, encryption code, decryption code, software or hardware or any other means required for his access to enable comprehension of the computerized data.

2.4 Communications and Multimedia Act 1998 (the "CMA")

The CMA gives the MCMC information gathering powers. Section 73 gives the MCMC the right to direct any person to provide them with information if the MCMC has reason to believe that the person has any information or document relevant to the performance of MCMC's powers and functions or is capable of giving any evidence which MCMC has reason to believe is relevant to the performance of its powers and functions.

Under section 77, MCMC may take and retain, for as long as necessary, any document provided to it pursuant to its information-gathering powers.

Under section 247, a magistrate may issue a warrant authorising any police officer not below the rank of Inspector or authorised officer to enter premises if it appears to the magistrate that there is reasonable cause to believe an offence under the CMA or its subsidiary legislation is being or has been committed on the premises or that those premises contain any evidence or thing which is necessary to an investigation. The authorised officer may enter the premises at a reasonable time with or without assistance, and if need be by force, and search for and seize any such evidence or thing. Section 247(8) states that if a search under section 247 indicates that there is any interference-causing equipment, radio apparatus or radiosensitive equipment, the authorised officer may direct that necessary steps be taken to ensure an interference-free environment.

Section 249 CMA gives the police officer and authorised officer conducting a search under the CMA (whether with or without a warrant) access to computerised data, however stored. "Access" is defined to include being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to comprehend computerised data, including access as defined under the CCA which provides the police with a wide range of rights in relation to accessing data.

Section 253 CMA makes it an offence to obstruct a search when a police officer or authorised officer is executing any duty imposed or conferred by law. The penalty for this offence is a fine not exceeding RM20,000.00 or imprisonment for a term not exceeding 6 months or both. If there is a court order or search warrant, the network operators and service providers may be liable for contempt of court if they refuse to assist.

2.5 General Consumer Code of Practice for the Communications and Multimedia. Industry (the "GCC")

The GCC requires a service provider, wherever possible to retain records of a customer's bill for a minimum period of one year. Material collected and recorded in relation to complaints handling processes is also to be retained by network operators and service providers for one year following the resolution of a complaint. However, the GCC also states that consumer data or information collected by service providers should not be kept longer than necessary.

The definition of "consumer" under GCC means a person who receives, acquires, uses or subscribes to services relating to communications and multimedia within the meaning of the CMA.

3. NATIONAL SECURITY AND EMERGENCY POWERS

Law enforcement and intelligence agencies have a number of special powers in times of emergency or for other special reasons. Below, we identify the common legislation invoked in such circumstances. Please note that there may be instances where emergency legislation is passed which is specific to a particular state within Malaysia. This is beyond the scope of this report.

3.1 Communications and Multimedia Act 1998 (the "CMA")

Under the CMA, a licensee shall, upon written request by the MCMC or any other authority, assist MCMC or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence or otherwise in enforcing the laws, including the protection of the public revenue and preservation of national security.

Under section 266, on the occurrence of any public emergency or in the interest of public safety, the Yang di-Pertuan Agong (the King of Malaysia) or the authorised Minister may:

(a) suspend the licence of any licensee, take temporary control of any network facilities, network service, applications service and/or content applications service owned or provided by a licensee in any manner as he deems fit;

(b) withdraw either totally or partially the use of any network facilities, network service, applications service and/or content applications service from any licensee, person or the general public;

(c) order that any communication or class of communications to or from any licensee, person or the general public relating to any specified subject shall not be communicated or shall be intercepted or detained, or that any such communication or its records shall be disclosed to an authorised officer mentioned in the order; or

(d) order the taking of possession of any customer equipment.

Under section 266(c), on the occurrence of any public emergency or in the interest of public safety, the Yang di-Pertuan Agong or the authorised Minister may order that any communication or class of communications to or from any licensee, person or the general public relating to any specified subject shall not be communicated or shall be intercepted or detained, or that any such communication or its records shall be disclosed to an authorised officer mentioned in the order.

3.2 Emergency (Essential Powers) Act 1979 (the "EEPA")

Section 2 EEPA gives the Yang di-Pertuan Agong the power to make any regulations whatsoever (the "Essential Regulations") which he considers desirable or expedient for securing public safety, the defence of Malaysia, the maintenance of public order and of supplies and services essential to the life of the community.

The Essential Regulations may, among other things, authorise the taking possession, control, forfeiture or disposal, on behalf of the Government of Malaysia, of any property or undertaking; or the acquisition, on behalf of the Government of Malaysia, of any property other than land; or authorise the entering and search of any premises; or provide for any other matter in respect of which it is in the opinion of the Yang di-Pertuan Agong desirable in the public interest that regulations should be made (sections 2(g), (h) and (o)).

3.3 Official Secrets Act 1972 (the "OSA")

Under section 6 OSA, any court may issue a search warrant to search for and seize a document, even though an offence under the OSA is not alleged, if it is satisfied that there is reasonable cause to believe a document contains matter or information prejudicial to the safety or interests of Malaysia and is directly or indirectly useful to a foreign power or to an enemy. "Document" is interpreted to include any other data embodied so as to be capable of being reproduced.

Section 12 OSA gives the Minister the power to require the production of certain messages sent to or from any place outside of Malaysia from any person who owns or controls any telecommunications device used for sending or receiving such messages (including the originals and transcripts of such messages and all other papers relating to the message). The request must be made by means of a warrant, and the messages should be provided to the Minister or any person named in the warrant.

There is also a duty under section 11 OSA to provide information when required to do so by the police, by any member of the armed forces or by an authorised public officer.

Sections 3(b) and (c) OSA stipulate that if, for any purpose prejudicial to the safety or interest of Malaysia, any person either makes any document or obtains, collects, records, publishes or communicates to another person any information which might be directly or indirectly useful to a foreign country, then they will be guilty of an offence punishable by life imprisonment. For the purpose of this section, "document" includes, in addition to a document in writing and part of a document:

(a) any map, plan, model, graph or drawing;

(b) any photograph;

(c) any disc, tape, sound track or other device in which sound or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and

(d) any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (as aforesaid) of being reproduced therefrom.

Under section 27 OSA, in the course of any court proceedings related to an offence under the OSA, an application may be made for a court order by the prosecution to exclude the public from any part of a hearing. The grounds required are that the publication of any evidence or statements made in the course of the proceedings would be prejudicial to the safety of Malaysia.

3.4 National Security Council Act 2016 ("NSCA")

Under the NSCA, the National Security Council ("Council") has the power, notwithstanding any other written law, to do all things necessary or expedient for or in connection with the performance of its functions including:

(a) to control and coordinate Government Entities on operations concerning national security; and

(b) to issue directives to any Government Entity on matters concerning national security.

Government Entity is defined to include:

(a) any ministry, department, office, agency, authority, commission, committee, board or council of the Federal Government, or of any of the State Governments, established under any written law or otherwise;

(b) any local authorities; and

(c) the Security Forces, defined as:

(i) the Royal Malaysia Police, the Royal Malaysia Police Volunteer Reserve and the Auxiliary Police referred to in the Police Act 1967;

(ii) the armed forces;

(iii) any force which is a visiting force for the purposes of Part 1 of the Visiting Forces Act 1960; or

(iv) the Malaysian Maritime Enforcement Agency established under the Malaysian Maritime Enforcement Agency Act 2004.

Under Section 18 of the NSCA, where the Council advises the Prime Minister that the security in any area in Malaysia is seriously disturbed or threatened by any person, matter or thing which causes or is likely to cause serious harm to the people, or serious harm to the territories, economy, national key infrastructure of Malaysia or any other interest of Malaysia, and requires immediate national response, the Prime Minister may, if he considers it to be necessary in the interest of national security, declare in writing the area as a security area. Upon a declaration being made under section 18, the Council may issue an executive order to the Director of Operations ("DO") or such Government Entities as the Council deems necessary in relation to the security area in the interest of national security. The DO has wide ranging powers in relation to security areas such as exclusion and evacuation of persons, establishing curfew and controlling movements of persons or any vehicle, aircraft or conveyance in and out of the security area.

Under Section 26, any member of the Security Forces may, without warrant and with or without assistance, stop and search any individual, vehicle, vessel, aircraft or conveyance in the security area if he suspects that any evidence of the commission of an offence against any written law is likely to be found and may seize any evidence so found. Under Section 34, any member of the Security Forces in a security area may use such force against persons and things as is reasonable and necessary in the circumstances to preserve national security.

Further, under Section 30(1), the DO or any person authorized by the DO may, if it appears to him to be necessary or expedient to do so in the interest of national security, or for the accommodation of any Security Forces, take temporary possession of any land, building or part of a building, or any movable property in any security area and may give such direction as appears to him necessary or expedient in connection with the taking of possession of that land, building or movable property.

Under Section 30(3), any land, building or movable property in temporary possession as per Section 30(1) above may be used for such purpose and in such manner by the DO or any person authorised by the DO as they think expedient in the interest of national security or for the accommodation of any Security Forces, notwithstanding any restriction imposed on the use thereof.

Section 17(2) of the NSCA also states that upon direction by the Council, any Government Entities or any person shall immediately make available any information or intelligence in its or his possession which relates to national security to the Council through the Director General. However, as the NSCA is a relatively new legislation, the scope and application of these sections have not yet been tested.

4. CENSORSHIP

4.1 Communications and Multimedia Act 1998 (the "CMA")

In general, the Minister and the MCMC are granted very wide powers to make determinations or declarations consistent with the objects and provisions of the CMA, the effect of which is that they may take control of or shut down network operators and service providers. Usually, the determinations or directives are issued pursuant to the CMA, which grants the Minister and the MCMC the power to issue determinations or directives on certain issues.

The CMA also contains several provisions regulating content and voluntary industry codes such as the Malaysian Communications and Multimedia Content Code (the "Code") (please see section 5.2 below) and General Consumer Code of Practice for the Communications and Multimedia Industry. While compliance with these voluntary industry codes by service providers is good practice but not mandatory, section 98 states that compliance with the voluntary code serves as a defence against any prosecution, action or proceeding of any nature taken against a person (who is subject to the voluntary industry code) regarding a matter dealt with in that code. It is also pertinent to point out that compliance with the General Consumer Code is part of the licence condition, and those who provide multimedia content may be required to comply with the Code. The MCMC may also direct any person to comply with both codes and failure to comply with such direction is an offence.

Section 211 of the CMA states that no content applications service provider shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person. Section 6 of the CMA defines content as any sound, text, still picture, moving picture, audio-visual or tactile representation, which can be manipulated, stored, retrieved or communicated electronically.

Under section 233, (a) a person who by means of any network facilities or network service or applications service knowingly makes, creates or solicits and initiates the transmission of obscene, indecent, false, menacing or offensive content with intent to annoy, abuse, threaten or harass any person; or (b) a person who knowingly by means of any network facilities or network service or applications service provides any obscene communication for commercial purposes or permits a network service or applications service under the person's control to be used for an activity described in (a), commits an offence.

Notwithstanding the above, Section 3 of the CMA, which states the objectives of the CMA provides that "nothing in the CMA shall be construed as permitting the censorship of the Internet".

4.2 Malaysian Communications and Multimedia Content Code (the "Code")

The Code provides guidelines and procedures for good practice in relation to the dissemination of online content to the public by service providers in the communications and the multimedia industry. The Code also regulates Internet Content Hosting Providers ("ICH") and Internet Access Service Providers.

Persons subject to the Code ("Code Subjects") who provide access to any electronic content (such as sounds, texts or pictures), but who do not control such content or have any knowledge of what it comprises, are deemed "innocent carriers". As such, they are not responsible for such content for the purposes of the Code. Nevertheless, this does not exempt them from the general measures in Part 6.0 of Part 5 where it expressly applies to them and, depending on the degree of control that Code Subjects may have over the online content, the specific measures in Parts 7.1 – 10.2 of Part 5 of the Code will have to be complied with (for example, to incorporate terms and conditions in their contracts such as the Code Subject's right to withdraw its hosting services where a user or subscriber contravenes Malaysian law).

The Code expressly states that ICHs are not required to do certain things, such as to block access by their users/subscribers to any material unless directed to do so by the Complaints Bureau, or monitor the activities of users and subscribers.

The Complaints Bureau is an arm of the Communications and Multimedia Consumer Forum, set up by the Malaysian Communications and Multimedia Commission to protect the rights of consumers in this sector. It deals with all complaints that relate to the Code.

4.3 Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (the "AMLA")

Section 6(3) stipulates that no person shall publish in writing or broadcast any information, including a report of any civil or criminal proceedings but excluding information published for statistical purposes by a competent authority or the Government, so as to reveal or suggest:

(a) that a disclosure was made under section 5; or

(b) the identity of any person as the person making the disclosure.

Section 5 relates to protection of informers and information relating to an offence under AMLA.

4.4 SEDITION ACT 1948

Section 10 states that where on the application of the Public Prosecutor it is shown to the satisfaction of a Sessions Court Judge that the making or circulation of a seditious publication:

(a) is or if commenced or continued would likely lead to bodily injury or damage to property;

(b) appears to be promoting feelings of ill will, hostility or hatred between different races or classes of the population of Malaysia; or

(c) appears to be promoting feelings of ill will, hostility or hatred between persons or groups of persons on the ground of religion,

the Sessions Court Judge shall make an order ("prohibition order") prohibiting the making or circulation of that seditious publication ("prohibited publication"). In relation to seditious publications by electronic means by a person who cannot be identified and which falls under any of the circumstances (a) to (c) above, the Sessions Court Judge shall make an order directing an officer authorized under the Communications and Multimedia Act 1998 to prevent access to such publication.

Subsection (1A) states that the prohibition order under subsection (1) shall:

(a) require every person having any copy of the prohibited publication in his possession, power, or control to deliver forthwith every such copy into the custody of the police; or

(b) in the case of a prohibited publication by electronic means:

(i) require the person making or circulating the prohibited publication to remove or cause to be removed wholly or partly the prohibited publication; and

(ii) prohibit the person making or circulating the prohibited publication from accessing any electronic device.

Bearing this in mind, some legal provisions may extend responsibility to network operators and service providers in relation to such laws even if the content is not actually provided or created by the network operators and service providers. These include abetting an offence punishable with imprisonment under section 116 of the Penal Code. In addition, under section 114A Evidence Act 1950, it is possible that the network operators and service providers may be presumed to be the publisher of the content contained on its customers' sites, unless the contrary is proved.

4.5 OTHER RELEVANT LEGISLATION

In relation to enforcement measures, under section 263 CMA, MCMC may request licensees to assist MCMC in preventing commission of an offence. This instruction may include blocking or removal of scam websites or websites with illegal content. Further, pursuant to section 51 CMA, MCMC may issue directions to "any person" regarding the compliance or non-compliance of the provisions of the CMA and its subsidiary legislations. This may include directions to comply or remedy non-compliance with provisions such as section 233 which sets out offences on improper use of network facilities or network services which appear to be wide enough to capture scam websites or websites with illegal content. MCMC largely works with the police and other law enforcement agencies to implement this, for example, through use of the Penal Code and sedition laws. The Penal Code, for example, provides for offences in relation to complaints about violent "hate" sites, including section 505 which makes it an offence to make, publish or circulate any statement, rumour or report:

(a) with intent to cause, or which is likely to cause, fear or alarm to the public, or to any section of the public whereby any person may be induced to commit an offence against the State or against the public tranquillity; or

(b) with intent to incite or which is likely to incite any class or community of persons to commit any offence against any other class or community of persons.

The penalty for an offence under this section is up to two years' imprisonment, a fine, or both.

The Penal Code also contains offences in relation to printing content containing slander or libel, and offences in relation to hosted sites which contain illegal content or encourage illegal acts.

5. OVERSIGHT OF THE USE OF POWERS

5.1 Communications and Multimedia Act 1998 (the "CMA")

Under the CMA, section 18 states that the Appeal Tribunal established under section 17 may review any matter on appeal, from a decision or direction of the MCMC, but not from a determination by the MCMC. Any decision by the Appeal Tribunal is final and binding on the parties to the appeal and is not subject to further appeal.

Section 120 provides that an aggrieved person or person whose interest is adversely affected by a decision or direction (but not a determination) of MCMC may appeal to the Appeal Tribunal for a review of the merits and the process of certain decisions or directions of the MCMC, unless the matter is not subject to an appeal to the Appeal Tribunal.

Section 121 provides for judicial review where a person is affected by a decision or other action of the Minister or MCMC and all other remedies provided under the CMA have been exhausted.

5.2 Security Offences (Special Measures) (Interception of Communications) Regulations 2012 under the SOSM (the "2012 Regulations")

Regulation 3 requires that a police officer who has acted under section 6(3) SOSM (interception without authorisation by the Public Prosecutor in urgent cases where immediate action is necessary) must submit a written report to the Public Prosecutor (the Attorney General) containing specified information detailed in the Second Schedule of the 2012 Regulations. The information required includes details of the officer making the interception, details relating to the individual whose communication was intercepted, the facts surrounding the investigation and the grounds for using interception.

5.3 Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (the "AMLA")

Section 31(4) requires the investigating officer, in the course of his investigation or search, to prepare and sign a list of all property, documents or information detained and state in the list the location in which or the person on whom, the property, document or information is found.

5.4 General power for Judicial Review ("JR")

Judicial review of the decision-making process of an authority exercising a power of a public nature by a court is available even if the executive/administrative decision is not open to any appeal or is expressed by the law to be 'final and conclusive'. Courts are not necessarily prevented from reviewing such acts or decisions.

The powers of the High Court in relation to JR are enshrined under the Specific Relief Act 1950 and the Courts of Judicature Act 1964. Grounds for JR include procedural impropriety, illegality, and irrationality in the decision-making process.

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

Restrictions on network operators and service providers

Under federal Malaysian law, there are no specific restrictions on publishing aggregate data relating to, for example, the volume of interceptions made in a single year. However, where not already set out in this report, the following laws could be employed to restrict such publication, in certain circumstances.

6.1 Communications and Multimedia Act 1998 (the "CMA")

The CMA provides confidentiality obligations in relation to documents or information considered to be confidential by the MCMC in the course of an investigation or trial or which relate to the affairs of the Appeal Tribunal (sections 26B, 61 and 63 CMA). MCMC may also issue a direction pursuant to section 51 CMA, requiring any persons including network operators or service providers to comply with such secrecy obligations. Such confidentiality obligations are open to judicial review under section 121.

In addition, under section 80 CMA, the MCMC is itself bound by certain obligations in respect of the publication of information. Section 80(3) CMA states that the MCMC must not publish any information disclosed to it if the publication would:

(a) disclose a matter of a confidential character;

(b) be likely to prejudice the fair trial of a person; or

(c) involve the unreasonable disclosure of personal information about any individual (including a deceased person).

However, the MCMC may publish an abstract relating to such information provided that the particulars in the abstract are not be arranged in any way which would compromise or prejudice the person providing such information.

Aggregate data published by government agencies.

6.2 Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (the "AMLA")

Section 6(3) AMLA (described in section 4.3 above) prevents the disclosure of certain information in legal proceedings, however, it exempts information published for statistical purposes by a competent authority or the government.

Generally, however, government agencies do not publish aggregate data in relation to the federal powers of interception, disclosure of data or censorship, as described in this report.

7. CYBERSECURITY

7.1 Communications and Multimedia Act 1998 ("the CMA")

The provisions under the CMA on cybersecurity are general. As such, the following sets out the general safeguards and remedies that may be used to ensure cybersecurity in Malaysia and should not be considered an exhaustive list.

Under Section 263 CMA, there is a general duty on licensees to use best endeavors to prevent their networks or services from being used in or in relation to the commission of any offence under Malaysian law.

The MCMC may direct a licensee or class of licensees to develop, in consultation with the authorities specified by the MCMC, a disaster plan for the survivability and recovery of any network facilities, network service, applications service or content applications service in case of a disaster, crisis or civil emergency as per Section 267.

There are also consumer codes and toolkits that have been prescribed in relation to cybersecurity. For example, there is the General Consumer Code ("the GCC"), which is a voluntary code issued by the Communications and Multimedia Consumer Forum of Malaysia ("the CFM"). The GCC states that service providers who create, maintain, use or disseminate individually identifiable information should take both appropriate measures to ensure its reliability and reasonable precautions to protect this type of information from loss, misuse or alteration. The GCC also states that service providers should take reasonable steps to ensure that third parties to whom they transfer such information are aware of these security practices, and take the same precautions to protect any such transferred information.

Security measures are also prescribed under the Internet Access Service Provider ("the IASP") Sub-Code issued under the GCC. The IASP Sub-Code states inter alia that service providers should have guidelines on how to implement security in their network and there must be some level of standard procedures to be followed. The code further states that the policy may cover items such as physical and environmental security, system access control and computer and network management. Moreover, it is important to note that whilst compliance with the GCC and the IASP Sub-Code is not mandatory, save for licensed service providers, the MCMC does have the power to direct any person to comply with the GCC. Any failure to comply with such direction constitutes an offence which would attract a fine of up to RM200,000.

Furthermore, failure to comply with any of the provisions of the CMA as described above may be considered a general offence which can incur liability of a fine not exceeding RM100,000 or 2 years' imprisonment or both, in addition to the forfeiture of anything seized.

"Determination" is defined in the CMA to mean "determinations made by MCMC under section 55 CMA" (which states that the MCMC may determine any matter specified in the CMA as being subject to MCMC's determination).

"Directions" are defined as directions issued by MCMC under section 51 CMA which provides that "The Commission may from time to time issue directions in writing to any person regarding the compliance or non-compliance of any licence conditions, and including but not limited to the remedy of a breach of a licence condition and the provisions of this Act or its subsidiary legislation."

Section 18 CMA provides that the Appeal Tribunal (which is established under Section 17) may review any decision or direction of the MCMC, but may not review any determination made by the MCMC. Therefore, under Section 120, an aggrieved individual whose interests have been adversely affected by a decision or direction (but not a determination) made by the MCMC may appeal to the Appeal Tribunal for a review of the merits of their case and the process taken by MCMC, unless the matter is not subject to an appeal to the Appeal Tribunal. Any decision that is made by the Appeal Tribunal is final and binding and not subject to further appeal. However under Section 121, an application for judicial review is available to an individual who is affected by a decision or other action of the Minister or MCMC where all other remedies provided under the CMA have been exhausted.

7.2 Personal Data Protection Act 2010 ("the PDPA")

The PDPA governs any processing of "personal data" completed in respect of a "commercial transaction" and applies if the "data user" (which is a concept equivalent to "data controller" in other jurisdictions) is:

(a) established in Malaysia and the personal data is processed by that person or any other person employed or engaged by that establishment; or

(b) not established in Malaysia, but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia.

Whilst the security requirements under the PDPA are general, more specific requirements are imposed under the Personal Data Protection Standards 2015 ("the PDP Standards") as discussed below.

The Security Principle (as set out in the PDPA and expanded by the PDP Standards) requires the data user to take steps to protect any of the personal data processed from loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction having regard to:

(a) the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;

(b) the place or location where the personal data is stored;

(c) any security measures incorporated into any equipment in which the personal data is stored;

(d) the measures taken to ensure the reliability, integrity and competency of personnel who have access to the personal data; and

(e) the measures taken to ensure the secure transfer of the personal data.

If the processing is carried out by a data processor on behalf of a data user, that data user is required for the purposes of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction to ensure that the data processor:

(a) provides sufficient guarantees in respect of the technical and organizational security measures governing the processing; and

(b) takes reasonable steps to ensure compliance with those measures.

There are also security requirements imposed under the Personal Data Protection Regulations 2013 ("the PDP Regulations"), which require data users to develop and implement a security policy for the purposes of the Security Principle described above. Such security policy must comply with the security standards set out from time to time by the Personal Data Protection Commissioner ("the Commissioner"). Data users must further ensure that the security standard, when processing the personal data, is complied with by any data processor that carries out the processing of the personal data on its behalf.

Additionally security standards can be found within the PDP Standards. The PDP Standards make recommendations for ensuring the security standard is maintained when dealing with personal data management, including suggestions such as that:

(a) the data user should have a backup/recovery system and the latest antivirus software to protect their clients data in the event of trespassing;

(b) the data user should be required to monitor the malware and scan the computer operating system with a schedule to prevent an attack on the electronically-kept data; and

(c) the electronic transfer of personal data should be restricted unless permitted (for related activity only) by the authorized officer.

It is the Commissioner who has the authority to carry out an inspection of:

(a) any personal data systems used by data users for the purpose of ascertaining information to assist the Commissioner in making recommendations to the relevant data user relating to the promotion of compliance with the provisions of the PDPA, in particular the Personal Data Protection Principles, by the relevant data user; and

(a) any personal data system used by data users belonging to a class of data users for the purpose of ascertaining information to assist the Commissioner in making recommendations to the class of data users to which the relevant data user belongs relating to the promotion of compliance with the provisions of this PDPA, in particular the Personal Data Protection Principles, by the class of data users to which the relevant data user belongs.

Non-compliance with the requirement to implement a security policy and to process personal data in accordance with any standards issued by the Commissioner may incur fines up to RM250,000 and/or two years' imprisonment. Also note that in certain circumstances companies' officers may also be found personally liable for offences under the PDPA in addition to the companies themselves.

The Commissioner, under the Ministry of Communications and Multimedia may, instead of convicting, serve an enforcement notice directing the data user to take certain steps to remedy any contraventions of the PDPA within a specified time period, and may order the cessation of the processing of personal data pending such remedy. However, failure to comply with an enforcement notice shall incur criminal liability in its own right.

Section 93 PDPA permits any person who is aggrieved by a decision of the Commissioner made in accordance with his authority under the PDPA to appeal the decision to the Appeal Tribunal. This section outlines in particular the appeal procedure to be used when appealing to the Appeal Tribunal in relation to a failure of the data user to comply with a data access or data correction request under Division 4 of Part II.

7.4 OTHER STATUTORY PROVISIONS

The section above does not cover the provisions of the Digital Signature Act 1997. It is also important to note that various other laws which are not specific to cybersecurity may also be applied in the context of cybersecurity, depending on the subject matter, such as theft, official secrets and national security offences.

8. CYBERCRIME

8.1 Computer Crimes Act 1997 (the "CCA")

The CCA generally protects against the misuse of computers, such as through hacking. The main offences discussed under the CCA and the penalties they attract are as follows:

CCA SECTION	Offence	Penalty
Section 3	Unauthorised access to computer material Described as causing a computer to perform any function with intent to secure access to any program or data held in any computer, the access of which the individual intends to secure is unauthorized and they are aware at the time when causing the computer to perform the function that this is the case.	A fine not exceeding RM50,000 or 5 years imprisonment or both.
Section 4	Unauthorized access with intent to commit or facilitate commission of further offence. Described as committing an offence referred to in Section 3 CCA (above) with intent: (i) to commit an offence involving fraud or dishonesty or which causes injury as defined in the Penal Code; or (ii) to facilitate the commission of such an offence whether by the offender or by any other person.	A fine not exceeding RM150,000 or imprisonment for a term not exceeding 10 years or both.
Section 5	**Unauthorised modification of the contents of any computer** Described as carrying out any act which an individual knows will cause unauthorized modification to the contents of any computer.	A fine not exceeding RM100,000 or imprisonment for a term not exceeding 7 years or to both. If the act is done with the intention of causing injury as defined in the Penal Code, the penalty is increased to a fine not exceeding RM150,000 and/or imprisonment for a term not exceeding 10 years.
Section 6	**Wrongful communication** Described as communicating directly or indirectly a number, code, password or other means of access to a computer to any person other than the person to whom the individual is duly authorized to communicate.	A fine not exceeding RM25,000 or imprisonment for a term not exceeding 3 years or both.

Note that the CCA shall, in relation to any person, whatever his nationality or citizenship, have effect outside as well as within Malaysia. Where an offence under the CCA is committed by any person in any place outside Malaysia, he may be dealt with in respect of such offence as if it was committed at any place within Malaysia. Moreover, the CCA shall apply if, for the offence in question, the computer, program or data was in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at the material time (s.9).

The only appeal mechanism available under the CCA is judicial review as discussed under cybersecurity above.

8.2 Communications and Multimedia Act 1998 (the "CMA")

Depending on the facts, the cybercrime in question may fall foul of several offences under the CMA. Some of the relevant offences and penalties that are dealt with under the CMA are as follows:

SECTION	Offence	Penalty
Section 231	Using any apparatus or device with the intent to obtain information regarding the contents, sender or addressee of any communication without an approval by a registered certifying agency.	A fine not exceeding RM50,000 or 2 years' imprisonment or both.
Section 233	Improper use of network facilities or network services. Described as where an individual, by means of any network facilities or network service or applications service knowingly makes, creates or solicits and initiates the transmission of, any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person; or initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with the intent to annoy, abuse, threaten or harass any person at any number or electronic address or, where a person knowingly: (a) by means of a network service or applications service provides any obscene communication for commercial purposes to any person; or (a) permits a network service or applications service under the person's control to be used for an activity described in paragraph (a).	A fine not exceeding RM50,000 or to 1 year's imprisonment or both, and a further fine of RM1,000 for every day during which the offence continues after the conviction.
Section 234	Unlawfully intercepting, attempting to intercept, or procuring interception by any other person of any communications and/or disclosing or attempting to disclose the contents of any communications, knowing or having reason to believe that the information was obtained through interception in contravention of the CMA, or using or attempting to use such contents.	A fine not exceeding RM50,000 or 1 year's imprisonment or both.
Section 235	Any willful, dishonest or negligent act or omission, to extend, tamper with, adjust, alter, remove, destroy or damage any network facilities or any part of them.	A fine not exceeding RM300,000 or to 3 years' imprisonment or both.
Section 236	Offences in relation to counterfeit access devices, unauthorized access devices and device-making equipment, with knowledge or intention to defraud. Note in particular Section 236(1)(d) which makes it an offence for a person, who knowingly or with intention to defraud, possesses, produces, assembles, uses, imports, sells, supplies or lets for hire, or has control or custody of any modified or altered equipment, device or apparatus or any hardware or software used for such modification or alteration, used to obtain unauthorized use of any network service, applications service or content applications service.	A fine not exceeding RM500,000 or 5 years' imprisonment or both.

Note that the CMA applies both within and outside Malaysia. As such, the CMA shall apply to any person beyond the geographical limits of Malaysia and her territorial waters if such person is a licensee under the CMA or provides relevant facilities or services under the CMA in a place within Malaysia.

Again, the only appeal mechanism available under the CCA is judicial review as discussed under cybersecurity above.

8.3 Other laws

As for cybersecurity, various other laws which are not specific to cybercrime may also be applied in the context of a cybercrime offence, depending on the subject matter (such as theft, sedition, official secrets and national security offences).

Law stated as at 21 February 2017.