LAW REFORM COMMISSION CONSULTATION:
CYBER-DEPENDENT CRIMES AND JURISDICTIONAL ISSUES

SUBMISSIONS

INTRODUCTION

The Law Society has reviewed the Consultation Paper issued in June 2022 by the Law Reform Commission on *Cyber-Dependent Crimes and Jurisdictional Issues* (the "Consultation Paper"). The responses and comments on the various recommendations put forward in the Consultation Paper are set out in the following.

A. ILLEGAL ACCESS TO PROGRAM OR DATA

Recommendation 1 (p.55 of the Consultation Paper)

Recommendation 1

The Sub-committee recommends that:

(a) Subject to a statutory defence of reasonable excuse, unauthorised access to program or data should be a summary offence under the new legislation.

(b) Unauthorised access to program or data with intent to carry out further criminal activity should constitute an aggravated form of the offence attracting a higher sentence under the new legislation.

(c) The proposed provisions of the new legislation should be modelled on sections 1, 2 and 17 of the CMA-EW.

Law Society's views:

1(a) We agree that, subject to a statutory defence of reasonable excuse, unauthorised access to program or data should be a summary offence under the new legislation.

1(b) We note the proposal to have an aggravated offence (paragraphs 2.107, 2.108 of the Consultation Paper). We in principle have no objection to this proposal, but would need to see more details on the criminal activities that trigger the aggravated offence as proposed. We expect these details are to be set out in a draft Bill, and reserve our comments.

1(c) No comments at this stage; we reserve our position until we are to review the draft Bill.

Recommendation 2 (p.61)

Recommendation 2

The Sub-committee invites submissions on whether there should be any specific defence or exemption for unauthorised access:

(a) If the answer is yes for cybersecurity purposes, in what terms? For example:

(i) should the defence or exemption apply only to a person who is accredited by a recognised professional or accreditation body?

(ii) if the answer to subparagraph (i) is yes, how should the accreditation regime work, e.g. what are the criteria for such accreditation? Should the accredited persons be subject to any continuing education requirements? Should Hong Kong establish an accreditation body (say, under the new cybercrime legislation or otherwise created administratively) that maintains a list of cybersecurity professionals so that, for instance, accredited persons who fail to satisfy the continuing education requirements may be removed from the list or not be allowed to renew their accreditation? Who outside the accreditation body (if any) should also have access to the list?

(iii) alternatively, if an accreditation regime is not preferred, should the new bespoke cybercrime legislation prescribe the requirements for putative cybersecurity professionals to invoke the proposed defence or exemption for cybersecurity

purposes? If so, what should these requirements be?

(b) Should the defence or exemption apply to non-security professionals?

Law Society's views:

2(a) We agree there should be specific defence or exemption for unauthorized access to programme or data.

(i) – (iii) Whether or not Hong Kong should have an accreditation regime (as proposed in the Consultation Paper) should be a policy matter for the HKSAR Government. There should be a full consultation by the Government with stakeholders and the industry.

At the moment, there is not any detailed *legal* analysis of this proposal in the Consultation paper e.g. as to how an accreditation scheme would impact upon prosecution or defence raised under the proposed offence (of unauthorized access). It is helpful to consider questions such as the following (which are not exhaustive): if an accreditation body is set up, would a certificate issued by the accreditation body serve as a defence to the charge under this offence? If yes, to what extent and how does it operate? Is that defence of certification separated from other defences an accused is entitled to? On the other hand, could law enforcement agencies go beyond the certificate issued by the accreditation body and investigate into the alleged unauthorized access?

2(b) At this stage we have no comments as to whether the defence or exemption applies to non-security professionals (see also our comments on Recommendation 8 below).

Recommendation 3 (p.62)

Recommendation 3

The Sub-committee recommends that the limitation period applicable to a charge for any of the proposed offences by way of summary proceedings should be two years after discovery of any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of

the offence, notwithstanding section 26 of the Magistrates Ordinance (Cap 227).

Law Society's views:

3. We agree that the relevant limitation period is two years.

B. ILLEGAL INTERCEPTION OF COMPUTER DATA

Recommendation 4 (p.99)

Recommendation 4

The Sub-committee recommends that:

(a) Unauthorised interception, disclosure or use of computer data carried out for a dishonest or criminal purpose should be an offence under the new legislation.

(b) The proposed offence should:

(i) protect communication in general, rather than just private communication;

(ii) apply to data generally, whether it be metadata or not; and

(iii) apply to interception of data *en route* from the sender to the intended recipient, i.e. both data in transit and data momentarily at rest during transmission.

(c) The proposed provision should, subject to the above, be modelled on section 8 of the Model Law on Computer and Computer Related Crime, including the *mens rea* (i.e. to intercept "intentionally").

Law Society's views:

4(a) We agree that unauthorized interception, disclosure or use of computer data carried out for a dishonest or criminal purpose should be an offence under the new legislation.

4(b)(i) We agree that the proposed offence of interception should protect communication in general, rather than just private communication.

4(b)(ii) This consultation question raises IT and technicalities issues which call for fuller explanation. On the other hand, there should be deliberation on the scope of the intended coverage of the proposed offence and the nature of the data proposed to be covered.

We express no views at this stage and reserve our position to comment, when we can have further (and technical) explanation, and/or we are to see the draft Bill.

4(b)(iii) We have no objection to the proposed offence be applied to interception of data *en route* from the sender to the intended recipient, i.e. both data in transit and data momentarily at rest during transmission, but we consider that the same *mens rea* requirement should be applicable to this interception offence, irrespective of whether the data is in transit or is momentarily at rest during transmission.

4(c) We have no views at this stage, and reserve our position to comment when we are to review the draft Bill.

Recommendation 5 (p.102)

Recommendation 5

The Sub-committee invites submissions on:

(a) Should there be a defence or exemption for professions who have to intercept and use the data intercepted in the course of their ordinary and legitimate business? If the answer is yes, what types of professions should be covered by the defence or exemption, and in what terms (e.g. should there be any restrictions on the use of the intercepted data)?

(b) Should a genuine business (a coffee shop, a hotel, a shopping mall, an employer, etc.) which provides its customers or employees with a Wi-Fi hotspot or a computer for use be allowed to intercept and use the data being transmitted without incurring any criminal liability? If the answer is yes, what types of businesses should be covered, and in what terms (e.g. should there be any restrictions on the use of the intercepted data)?

Law Society's views:

5(a) We agree there should be a defence or exemption for professions who have to intercept and use the data intercepted in the course of their ordinary and legitimate business. As to what types of professions are to be covered by the defence or exemption, that should be a policy matter for the HKSAR Government.

5(b) We hold no strong views as to whether a genuine business (a coffee shop, a hotel, a shopping mall, an employer, etc.) which provides its customers or employees with a Wi-Fi hotspot or a computer for use be allowed to intercept and use the data being transmitted without incurring any criminal liability.

If a business is allowed to intercept, disclose or use the data being transmitted, we are of the view that those should not be for a dishonest or for a criminal purpose. We repeat our comments in paragraph (a) under Recommendation 4 in the above.

As to what types of business should be covered and in what terms, again that should be a policy matter for the HKSAR Government.

C. ILLEGAL INTERFERENCE OF COMPUTER DATA

Recommendation 6 (p.136)

Recommendation 6

The Sub-committee recommends that:

(a) Intentional interference (damaging, deletion, deterioration, alteration or suppression) of computer data without lawful authority or reasonable excuse should be an offence under the new legislation.

(b) The new legislation should adopt the following features under the Crimes Ordinance (Cap 200):

(i) the *actus reus* under section 59(1A)(a), (b) and (c);

(ii) the *mens rea* under section 60(1) (which requires intent or recklessness, but not malice);

(iii) the two lawful excuses under section 64(2), while preserving any other lawful excuse or defence recognised by law; and

(iv) the aggravated offence under section 60(2).

(c) The above provisions regarding "misuse of a computer" should be separated from the offence of criminal damage and adopted in the new legislation, while deleting section 59(1)(b) and (1A) of the Crimes Ordinance (Cap 200).

Law Society's views:

6(a) We agree that intentional interference (damaging, deletion, deterioration, alteration or suppression) of computer data without lawful authority or reasonable excuse should be an offence under the proposed legislation.

6(b)(i) We have no comments on the proposed *actus reus*, and reserve our position to comment when we are to see the draft Bill.

6(b)(ii) It must be obvious that for someone who is mindful of interfering with data stored in a computer, that person must have the intention to do so. He would have to plan ahead, procure the necessary tools (software) and avail himself of the opportunities. He would have to gain access to the computer, get hold of those data, and alter or delete those data. The above calls for a *deliberate* chain of actions. We understand the rationale for the *mens rea* requirement of "intent" for this proposed offence and have no objection.

However, it is not clear to us as to why the proposed *mens rea* requirement of "recklessness" is appropriate or relevant, noting that :

(A) Recommendation 6 itself refers to "*intentional interference of computer data*" (see sub-paragraph (a) of Recommendation 6 in the above);

(B) the meaning of "interfering" under the proposal are as follows (paragraph 4.3 of the Consultation Paper):

"*(a) Modifying a file saved in a computer after accessing it without authority.*

(b) Interfering with data by means of a computer virus that can, say, delete specified data stored in an infected computer."

The above must be *premediated*.

The explanation in the Paper (paragraph 4.89 of the Consultation Paper) does not help.

6(b)(iii) – (iv) We hold no views at this stage.

6(c) We have no objection.

D. ILLEGAL INTERFERENCE OF COMPUTER SYSTEM

Recommendation 7 (p.162)

Recommendation 7

The Sub-committee recommends that:

(a) The proposed provisions regarding the illegal interference of computer data and computer system should be phrased in the same way.

(b) Sections 59(1A) and 60 of the Crimes Ordinance (Cap 200) suffice to prohibit the illegal interference of computer system and should also be adopted in the new legislation.

(c) The new legislation should retain the breadth of the existing law and should not be too restrictive, while clarifying the phrase "misuse of a computer" as appropriate (e.g. incorporating the notion "impair the operation of any computer").

(d) The proposed offence of illegal interference of computer system should, for example, apply to a person who intentionally or recklessly:

(i) attacked a computer system whether successful or not (criminal liability should not depend on the success of an interference);

(ii) coded a software with a bug during its manufacture; and

(iii) changed a computer system without authorisation, knowing that the change may have the effect of preventing access to, or proper use, of the system by legitimate users.

Law Society's views:

7(a) – (d) For the various recommendations in the above, we have the following comments.

1) The proposal is to transpose section 59(1A) and 60 of the Crimes Ordinance Cap 200 to the proposed legislation. Section 59(1A) and 60 were enacted respectively in 1993 and 1972. Noting that these offences were formulated 30 – 40 years ago, and that they are in essence intended to cover physical damage, a deliberation as to why and if so how the elements of these offences are applicable to cyber-crimes would be helpful.

2) Section 60 (but not section 59(1A)) alludes to the element of "recklessness" as an element of the proposed offence. In this regard, we note the following in the Consultation Paper,

> *"5.5 Where a computer system has been subject to what appears to be a DDOS attack[1], whether the parties who collectively caused the result intended to attack the system may be a crucial factual issue. For instance, an emergency hotline service that operates through a computer system may be jammed by a large number of incoming calls. One must differentiate between many people coincidentally dialling the hotline at the same moment, and someone commanding hundreds or thousands of computers to dial the hotline in a concerted*

[1] "DDOS attack" is defined in the Consultation Paper as "[t]he intentional paralysing of a computer network by flooding it with data sent simultaneously from many individual computers" (see para 5.3)

manner. The latter scenario is more comparable to a DDOS attack.

5.6 Apart from DDOS attack, a new way to interfere with a computer system – called slow attack – has emerged. A DDOS attack is analogous to the situation where many customers place orders in a restaurant at the same time, whereas one can liken a slow attack to a customer using many small-denomination coins to pay a bill in the restaurant, thus disrupting normal services. While a DDOS attack causes the target computer system to generate a large amount of log record, a slow attack may only keep the target computer system engaged for a prolonged period."

There is in the Consultation Paper a short passing reference to section 250 (2)(c) of the New Zealand Act on use of 'recklessness'[2]. Apart from the above, these is no analysis in the Consultation Paper as to why it is considered to be appropriate to include the element of 'recklessness' in this offence. Questions on criminal liability (if any), and the necessary legal basis therefor, of a reckless flooding of a computer system[3] deserve more comprehensive analysis.

3) There must be careful consideration in the above as, *prima facie*, inclusion of the element of 'recklessness' in the offence widens the scope of the offence.

Recommendation 8 (p.164)

Recommendation 8

The Sub-committee invites submissions on:

(a) Should scanning (or any similar form of testing) of a computer system on the internet by cybersecurity professionals, for example, to evaluate potential security vulnerabilities without the knowledge or authorisation of the owner of the target computer, be a lawful excuse for the proposed offence of illegal interference of computer system?

[2] See paragraph 5.40 to 5.42 of the Consultation Paper.

[3] As in the case of fans fighting online to snap up concerts tickets

(b) Should there be lawful excuse to the proposed offence of illegal interference of computer system for non-security professionals, such as:

(i) web scraping by robots or web crawlers initiated by internet information collection tools, such as search engines, to collect data from servers without authorisation by connecting to designated protocol ports (e.g. ports as defined in RFC6335);[4] and/or

(ii) scanning a service provider's system (which has the possibility of abuse or bringing down the system) for the purpose of:

(1) identifying any vulnerability for their own security protection, for example, whether the encryption for a credit card transaction is secure before they, as private individuals, provide their credit card details for the transaction; or

(2) ensuring the security and integrity of an Application Programming Interface offered by the service provider's system?

Law Society's views:

8(a) This proposal (scanning by professional be construed as a lawful excuse) circles back to the previous discussion on whether there should or should not be an accreditation and/or certification system to oversee and to regulate professionals. The accreditation/ certification / regulation of professionals should be a policy matter for the HKSAR Government. We repeat our comments on Recommendation 2 above.

8(b) The above observations apply *mutatis mutandis* to the questions raised in Recommendation 2(b), in relation to 'non-security professionals' (the definition of which is lacking). See therefore our comments on Recommendation 2(b) above.

There is on the other hand little or no discussion in the Consultation Paper on the proposal to criminalize activities of

[4] Information about RFC6335 is available on the website of the Internet Engineering Task Force, at https://datatracker.ietf.org/doc/rfc6335/ (accessed on 3 May 2022).

web scraping by robots or web crawlers. Absent clarification on the above, it is premature to comment on proposed 'lawful excuse' put forward in the paper.

E. MAKING AVAILABLE OR POSSESSING A DEVICE OR DATA FOR COMMITTING A CRIME

Recommendation 9 (p.194)

Recommendation 9

The Sub-committee recommends that:

(a) Knowingly making available or possessing a device or data (irrespective of whether it is tangible or intangible, e.g. ransomware, a virus or their source code) made or adapted to commit an offence – i.e. not necessarily cybercrime – should be a basic offence under the new legislation, subject to a statutory defence of reasonable excuse.

(b) The *actus reus* of the proposed offence should cover both the supply side (such as production, offering, sale and export of a device or data in question) and the demand side (such as obtaining, possession, purchase and import of a device or data in question).

(c) The proposed offence should apply to:

(i) a device or data so long as its primary use (to be determined objectively, *regardless of* a defendant's subjective intent) is to commit an offence, *regardless of* whether or not it can be used for any legitimate purposes; and

(ii) a person who believes or claims that the device or data in question *could be* used to commit an offence, irrespective of whether that is true or not.

(d) Knowingly making available or possessing a device or data (irrespective of whether it is tangible or intangible, e.g. ransomware, a virus or their source code):

(i) which is, or is believed or claimed by the perpetrator to be, capable of being used to commit an offence; and

(ii) which the perpetrator intends to be used by any person to commit an offence

should constitute an aggravated offence under the new legislation, subject to a statutory defence of reasonable excuse.

(e) The proposed provisions should be modelled on section 3A of the CMA-EW as well as sections 8 and 10 of the CMA-SG.

Law Society's views:

9(a) – (e)

We have the following comments. To assist the discussion, we have provided some highlights (underlined) in the above box.

1) The proposed offences as currently framed are extremely wide, with a low threshold for prosecution.

2) Under the proposal, *possessing* data (tangible or intangible) which may be *adapted* to commit a crime (*not necessarily cyber-crime*) would be an offence. A person who *believes* that the data in question could be used to commit an offence would be caught.

3) Therefore, under the proposal, if a party (A) passes to another party (B) a digital private photo of a celebrity having intimate moments with a third party, B in theory could be guilty of the offence, as (i) that photo can be used to blackmail the celebrity, and (ii) B believes that that photo *could be* used to commit the offence of blackmail.

4) It matters not whether B's belief is reasonable or not; it also does not matter whether the blackmailing is true or not.

5) The offence would be committed so long as the data "could be" used to commit that offence. The prosecution needs not prove that the data *has been* used to commit the offence.

6) The above could have wide implications as, e.g., B in the example is a private investigator, and A is his client. The client passes to the private investigator the digital photos for advice. The private investigator potentially could be charged for the

proposed offence. This is worrying - in this example the private investigator would be put at risks at prosecution, when he is receiving data only to do his job legitimately. Why should he be put at risk for prosecution?

7) We are also concerned about juxtaposition of the wordings in the section. The way the proposed offence is framed is indigestible.

8) Recommendation 9(c)(i) disregards both a defendant's intent and the fact that a device could be used of a legitimate purpose. These wordings greatly impinge the defence of reasonable excuse.

9) As the Recommendation disregards a defendant's subjective intent and the legitimate purpose, a person claiming harmless items could be used to commit an offence could in theory commit this offence itself. It is difficult to know whether that is an acceptable formulation before we are to see the draft Bill. In any event, this Recommendation must be scrutinized very carefully.

10) The Consultation Paper uses the analogy of "supply" and "demand" for the proposal. We have no objection to employ the concept of "supply" in the analysis, but the reference to the concept of "demand" is not helpful. The concept of "demand" carries with it the requirement of requesting. Whether this is the intention for this offence is not explained in the Consultation Paper. Without any details or explanations in the paper, it seems to us that the concepts such as "acquisition" would be more relevant in the consideration of this offence, in place of "demand" (as a concept).

11) On the "demand side" of this Recommendation, reference has been made to "possession" (of a device or data in question). (see sub-paragraph (b) of this Recommendation). As possession offences merit different considerations, we suggest the offence of "possession" under the proposal be framed as an offence <u>separate</u> from other offences proposed.

It is not at all unusual to have a separate possession offence. An analogy could be the separate offences of "trafficking" dangerous drugs and "possessing" dangerous drugs.

12) If this proposal is to be further pursued, all the above must be considered carefully.

Recommendation 10 (p.197)

Recommendation 10

The Sub-committee invites submissions on:

(a) Whether there should be a defence or exemption for the offence of knowingly making available or possessing computer data (the software or the source code), such as ransomware or a virus, the use of which can only be to perform a cyber-attack?

(b) If the answer to paragraph (a) is "yes",

(i) in what circumstances should the defence or exemption be available, and in what terms?

(ii) should such exempted possession be regulated, and if so, what are the regulatory requirements?

Law Society's views:

10(a) – (b)

The question posed relates to the possible use of ransomware or virus for education, research, or security stress-tests. In response, we refer to our comments on "certification" (Recommendation 2) and "professionals" (Recommendation 7) in the above.

F. CRITERIA FOR THE HONG KONG COURT TO ASSUME JURISDICTION

Recommendation 11 (p.230)

Recommendation 11

The Sub-committee recommends that, in respect of the proposed offence of illegal access to program or data, Hong Kong courts

should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

(b) the victim (the target computer's owner, the data's owner, or both) is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong;

(c) the target computer, program or data is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong,

subject to a requirement that, in respect of a perpetrator charged with the summary offence on the basis of his or her act done outside Hong Kong, such act, either alone or together with other such act(s), omission(s) or event(s) the proof of which is required for conviction of the Hong Kong offence, must constitute a crime in the jurisdiction where it was done.

Law Society's views:

11(a) – (d)

We agree, subject to a further review after the sight the draft Bill.

Recommendation 12 (p.232)

Recommendation 12

The Sub-committee recommends that, in respect of the proposed offence of illegal interception of computer data, Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

(b) the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on

business in Hong Kong;

(c) the target computer, program or data is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong.

Law Society's views:

12(a) – (d)

We agree, subject to a further review after the sight of the draft Bill.

Recommendation 13 (p.233)

Recommendation 13

The Sub-committee recommends that, in respect of the proposed offence (including its basic and aggravated forms) of illegal interference of computer data, Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

(b) the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong;

(c) the target program or data is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong.

Law Society's views:

13(a) – (d)

We agree, subject to a further review after the sight of the draft Bill.

Recommendation 14 (p.234)

Recommendation 14

The Sub-committee recommends that, in respect of the proposed offence (including its basic and aggravated forms) of illegal interference of computer system, Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

(b) the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong;

(c) the target computer is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong.

Law Society's views:

14(a) – (d)

We agree, subject to a further review after the sight of the draft Bill.

Recommendation 15 (p.236)

Recommendation 15

The Sub-committee recommends that, in respect of the proposed offence of making available or possessing a device or data for committing a crime, Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other

such act(s), omission(s) or event(s) occurred elsewhere, e.g. a person physically in Hong Kong making available on the dark web, a device or data for committing an offence;

(b) the perpetrator is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong; or

(c) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong.

Law Society's views:

15(a) – (c)

We agree, subject to a further review after the sight of the draft Bill.

G. SENTENCING

Recommendation 16 (p.246)

Recommendation 16

The Sub-committee recommends that:

(a) In respect of the proposed offence of illegal access to program or data, an offender should be liable to the following maximum sentences:

(i) for the summary offence, imprisonment for two years; or

(ii) for the aggravated offence, imprisonment for 14 years on conviction on indictment.

(b) In respect of the proposed offence of illegal interception of computer data, an offender should be liable to imprisonment for two years on summary conviction and 14 years on conviction on indictment.

(c) In respect of each of the proposed offences of illegal interference of computer data and illegal interference of computer system, an offender should be liable to the following maximum sentences:

(i) for the basic offence, imprisonment for two years on summary conviction and 14 years on conviction on indictment; or

(ii) for the aggravated offence, imprisonment for life.

(d) In respect of the proposed offence of making available or possessing a device or data for committing a crime, an offender should be liable to the following maximum sentences:

(i) for the basic offence, imprisonment for two years on summary conviction and seven years on conviction on indictment; or

(ii) for the aggravated offence, imprisonment for 14 years on conviction on indictment.

Law Society's views:

16(a) & (b) We have no comments at this stage.

16(c) The sentencing for this aggravated offence is imprisonment for life. That is different from the sentencing of other aggravated offence (which is 14 years). The rationale put forward for this sentence is set out in paragraph 8.20 of the Paper:

> *"8.20 To maintain consistency with the offence of criminal damage, we suggest adopting the maximum sentence now prescribed by section 63(1) of the Crimes Ordinance (Cap 200), i.e. imprisonment for life, for the proposed aggravated offences of illegal interference of computer data and that of computer system."*

(See also paragraph 8.14 (d) of the Consultation Paper)

The justification seems to be a reference to and reliance upon section 63, Cap 200. Section 63 is on arson. This offence directly causes grave bodily harm. People's life is at stake. The Consultation Paper has not explained the relevancy or equivalence of section 63 Crimes Ordinance to the proposed aggravated offence (of illegal interference of computer data and computer system), in terms of gravity of the harm potentially caused, or otherwise. On the other hand, we are

not aware of any life imprisonment sentence being handed down for criminal damage.

The Consultation Paper has also not set out what aggravating factors are to be introduced for this offence (to justify this level of sentence). At the moment, we have no idea on the possible circumstances the Prosecution would urge the Court to hand down life sentence for this offence (e.g. how serious the interference has to be, for a life sentence to be imposed).

An elaboration on all the above would be helpful.

CONCLUSION

We welcome the Law Reform Commission's Consultation Paper, which initiates discussions for legislation against cybercrimes. There are a number of issues which in our views merit more in-depth deliberation, and we look forward to further discussion thereon.

The Law Society of Hong Kong
27 September 2022