FINTECH ASSOCIATION
OF HONG KONG

# *Response to the Consultation Paper on Cyber-dependent Crimes and Jurisdictional Issues*

# CONTENTS

The FinTech Association of Hong Kong (FTAHK) is a **member-driven, independent, not-for-profit, & diverse** organisation that is the voice of the FinTech community in Hong Kong. It is organised and led by the community, for the community, through a series of committees and working groups.

Our objective is to promote Advocacy, Communication and Education in the wider FinTech ecosystem.

**Build the community.**

**Be the #superconnector.**

# A. FOREWORD

The Law Reform Commission Sub-Committee on Cybercrime (the "**LRC**" and such Sub-Committee, the "**Sub-Committee**") released a Consultation Paper on Cyber-Dependent Crimes and Jurisdictional Issues in June 2022[1] (the "**Consultation Paper**"), inviting views from members of the public on the recommendations proposed to address five forms of cyber-dependent offences, namely: (i) illegal access to program or data; (ii) illegal interception of computer data; (iii) illegal interference of computer data; (iv) illegal interference of computer system; and (v) making available or possessing a device or data for committing a crime. The need for review of Hong Kong's existing legislation around cybercrimes was highlighted following enactment of the National Security Law on June 30, 2020.

The Consultation Paper sets out the LRC's thinking on the regulatory approach to be adopted when considering legislative change. As stated in section 12, the LRC's guiding principles are: to balance; (i) the right of netizens and interests of persons in the information technology industry and (ii) protection of the public interest and right not to be disturbed or attacked when using and operating their computer system."

Financial Services are a key industry for Hong Kong, with the latest reported quarterly GDP for "Financing and Insurance" services being HKD157,170m (23.5% of overall second quarter 2022 GDP of HKD 668,198m)[2]. Whilst the financial services sector has increasingly adopted and incorporated technology into its operations over the last fifty years, it is one of a number of industries that are increasingly becoming technology businesses first. As the first of the HKMA's strategy objectives for 2025 indicates, "All banks go fintech" is core to maintaining Hong Kong's role as a leading international finance centre.[3]

The FTAHK is a not-for-profit industry organisation that represents "FinTech" and has over 900 members representing approx. 300 firms and is the largest and most relevant FinTech association in Hong Kong. Our wide-ranging membership comprises of global and domestic FinTechs, international, regional and Hong Kong based Financial Institutions, Technology Service Providers, Consultancies, Law Firms, Academia, and Students.

We are grateful to have the opportunity to respond to this Consultation Paper based on input from our members.

The FTAHK welcomes the opportunity to discuss any of the feedback provided in future follow-up sessions with the LRC.

19 October 2022

FinTech Association of Hong Kong
https://ftahk.org
generalmanager@ftahk.org

[1] https://www.hkreform.gov.hk/en/docs/cybercrime_e.pdf
[2] https://www.hkma.gov.hk/eng/data-publications-and-research/data-and-statistics/economic-financial-data-for-hong-kong/#financialSector
[3] https://www.hkma.gov.hk/eng/news-and-media/press-releases/2021/06/20210608-4/

# B. EXECUTIVE SUMMARY

The FTAHK welcomes the opportunity to provide feedback on the recommendations proposed to address five forms of cyber-dependent offences, namely: (i) illegal access to program or data; (ii) illegal interception of computer data; (iii) illegal interference of computer data; (iv) illegal interference of computer system; and (v) making available or possessing a device or data for committing a crime. As can be seen in the detailed responses to the questions raised in the Consultation Paper, we wish to highlight two themes, which we believe to run across the Consultation Paper:

(i) The Guiding Principles adopted by the LRC are too narrowly framed and do not reflect the full impact of technology in Financial Services and other industries normal practice; and

(ii) The absence of intent will criminalise normal activities of businesses dependent on technology. As such, the current proposals may have an adverse impact not only on such businesses and their related industries, but also on the protection of the public interest. This concern arises from the absence of the common law principles of *mens rea* in deciding whether a crime has been committed (i.e., for the act to be a crime, one must have the guilty mind (intent) in addition to the act).

*Guiding Principles need to be broadened in scope*

The Consultation Paper sets out the LRC's thinking on the regulatory approach to be adopted when considering legislative change. As stated in section 12, the LRC's guiding principles are: to balance; (i) the right of netizens and interests of persons in the information technology industry and (ii) protection of the public interest and right not to be disturbed or attacked when using and operating their computer system."

The FTAHK is of the view that these guiding principles are too narrow: 'computer systems' are integral to the operation of the financial services industry and increasingly nearly all other industries in Hong Kong. We believe that the guiding principles should look to balance the need to govern the software systems on which Hong Kong businesses/ organisations run to provide services to the public, against the desire to protect the public's safety and ability to go about their normal life. We find the LRC's use of the phrase *'netizens and IT industry'* to be out of touch with the reality of the reliance on software to run all aspects of public and private organisations.

All businesses are running on (and therefore critically dependent on) technology. The financial services industry, in particular, can be seen as a technology business operating in the domain of finance. Securing these services (which are highly complex and open to layers of vulnerabilities) requires the possession and active use of tools and approaches that sections of the proposals plan to criminalise. We note that accidents and/or negligence, as well as bad actors, can lead to the exposure of sensitive/ personal identifiable information and threaten the normal operations of the public and society.

Referencing the above, an example of bad actors that need to be protected against include the ransomware attacks on hospitals around the world, either by organised criminal groups and/or state actors[4][5].

An example of accidents/ negligence closer to Hong Kong is the exposure of highly sensitive information held by the IPCC[6] . We note that the loss of this data was only discoverable through use of an 'unauthorised' google web-crawler, a service which would be criminalised if the recommendations were to be adopted wholesale without amendment.

It is the position of the FTAHK that the Guiding Principles should be expanded and re-framed towards achieving a balance between, (i) the right of legitimate businesses critically dependent on technology to adopt best practices to protect the safety and integrity of their systems against organised crime and accidental exposure; and (ii) protection of the public interest generally in not being disturbed or attacked when using services dependent on computer systems.

### *Test of 'intent' needs to be re-introduced*

By proposing to criminalise (without considering an alleged offender's intent) the very tools and approaches that legitimate businesses rely on to protect the technology infrastructure upon which the Hong Kong public relies, it would appear that the proposals will have the effect to criminalise the 'normal' security practices of *bona fide* in-house teams, security professionals, 'white-hat' hackers and bounty program responders. The FTAHK is therefore of the opinion that it is essential to re-introduce the test of 'intent' of an activity when assessing whether a crime has been committed as a means to create the necessary balance of interests, and that the level of 'intent' (e.g., purposely, knowingly recklessly and negligently) should reflect the level of criminal culpability.

### *Impact on Hong Kong Financial Services and other industries*

The current recommendations would primarily adversely affect the risk environment for how businesses operate, potentially exposing the public to a less secure environment. Commercially the recommendations would reduce Hong Kong entities regional and international competitiveness. We note that implementation of the recommendations in their current form would be a departure from international legal norms in the industry and corresponding relevant peer jurisdictions – this may then have a secondary adverse impact on the HKMA and Government's ability to meet their stated policy desire(s) of advancing Hong Kong as an international Finance and IT hub. We also note that attracting finance and technology talent to Hong Kong may also prove to be difficult.

[4] Around the world, attacks on public services are rife – see https://www.theguardian.com/world/2021/may/14/ransomware-attack-disrupts-irish-health-services for an example of an attack on the Irish health system.
[5] https://www.infosecurity-magazine.com/news/healthcare-ransomware-last-year/
[6] https://www.legco.gov.hk/yr05-06/english/panels/itb/papers/itb0317cb1-1096-5e.pdf

Overall, we are supportive of enhanced legislation to protect the public. However, the FTHAK suggests that the guiding principles be re-framed, and the test of intent be re-introduced as a means of avoiding any unintended consequences of the current recommendations, which may ultimately increase the risk of the public when they are engaged in online activities.

# C. RESPONSES TO QUESTIONS

## C.1 Illegal Access to Program or Data

**Recommendation 2:** Should there be any specific defence or exemption for unauthorised access?

The FTAHK recognises that the cybercrime regime in Hong Kong is due an update (given the long passage of time since promulgation of the current legislation governing cybercrimes, and the significant technological and societal developments of the last two decades) and is appreciative of the depth of research that the LRC has undertaken prior to formulating its recommendations.

However, we would like to highlight to the LRC that the current form of the proposals, if implemented, would represent a departure from international norms within the cybersecurity industry, as compared to relevant peer legal jurisdictions. Whilst we are cognisant of the desire to implement legislation that is supportive of other security legislation (notably the National Security Law), we believe that implementation of the recommendations may make it difficult to attract information technology ("**IT**") talent to Hong Kong and, concomitantly, adversely affect the risk profile of the city for businesses (particularly those heavily reliant on IT) to operate, as well as impact their regional and international competitiveness. As has been widely reported in the media, the government has identified development of the FinTech industry as a key prong for the future growth of Hong Kong, and we are concerned that the present form of recommendations may serve to stymie that growth.

Whilst we agree with the position of the LRC that it is difficult to justify permission of conduct in cyberspace that would be prohibited in the physical world, the FTAHK would recommend that this thinking not be absolute, and that a degree of flexibility built into the offence, i.e., not adopting a position of strict liability and laying the burden on the prosecution to prove that the defendant had the *mens rea* at the time of the offence. This we feel would obviate the need for a specific defence and ensure that Hong Kong remains in line with its peers.

That being said, were legislation to be drafted in the form of the present recommendations, we propose that the LRC does allow for specific defences or exemptions, for example in situations where an individual or company is engaged to test, or validate, the strength of a client's security controls. We would also like to draw the LRC's attention to the concept of "bug bounty programs", where individuals are rewarded for identifying and reporting bugs, particularly those pertaining to security exploits and vulnerabilities[7]. Participants in these programs may be individual cybersecurity enthusiasts who have altruistic goals to improve security and make interacting with technology a safer activity, as well as corporations who have been paid to identify (and later remediate) potential security deficiencies.

In these instances, an argument can be made that individuals who have obtained unauthorised access are, in fact, acting in the public good as they are providing a service to the relevant company/ website/ network operator etc. What is

[7] https://en.wikipedia.org/wiki/Bug_bounty_program

important here is the intention behind the actions leading to the unauthorised access, and we would urge the LRC to consider integration of the four different levels[8] of *mens rea* when finalising drafting of the proposed offence.

(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 sub-paragraph (i) is yes, how should the accreditation regime work, e.g., what are the criteria for such accreditation? Should 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?

The FTAHK is of the view that the intent behind these activities should be considered when analysing whether any offence has, in fact, taken place.

As provided above, the FTAHK is of the view that there should not be a specific defence or exemption for unauthorised access. Were such a defence or exemption to be adopted, we do not believe that any defence or exemption should only apply to a person who is accredited by a recognised professional or accreditation body. The IT and cybersecurity fields are not regarded in the same vein as the legal and medical professions, where accreditation is viewed as a "license to practice", versus external proof of expertise.

Adopting an accreditation regime in Hong Kong would serve to make the city an outlier compared to its peers, and as stated above, likely result in additional difficulties in recruiting talent within this sector to either work in Hong Kong, or to work for Hong Kong companies. This may then have the unintentional effect of limiting the degree of protection available to local netizens, as there may be a dearth of cybersecurity professionals able to operate legally within the city.

The FTAHK also notes that there may be practical difficulties of imposing an accreditation regime: the recommendation presumes that there may be a set of recognised bodies across jurisdictions that are able to provide

[8] Namely, (i) purpose; (ii) knowledge; (iii) recklessness; and (iv) negligence.

the relevant accreditation. Absent the People's Republic of China, the FTAHK notes that jurisdictions that have made inroads into the development of a cybersecurity accreditation system have done so for industry recognition purposes, and not to form the basis of a defence to a criminal offence. A review of industry sources from the United Kingdom and Singapore shows that there is no link between an individual's accreditation status and the availability of a defence to, or even for an accreditation requirement for an individual to practice cybersecurity. We further note that the link provided within the Consultation Paper is to an industry training program, rather than a formal accreditation scheme.

As an additional consideration, the FTAHK notes that given the cross-border nature and impact of IT, we foresee a need to determine a global list of recognised bodies/ accredited institutions, which may serve to limit the talent pool available to employers in Hong Kong as some of the best candidates for the job may not have ready access to an accreditation centre in their jurisdiction.

In addition, the drive by Hong Kong for an accreditation system would essentially require a transition process for all existing IT professionals. For some individuals/ companies within the IT industry, this may be an unnecessary burden as an ancillary component to their main job function may trigger the need for accreditation. An example of this is in the field of software engineering: in the course of developing software, software engineers go through phases of "vulnerability testing" – this is, in essence, a form of cybersecurity analysis (hacking), but there is no malintent in this process.

As a final point to note, we are of the view that the recommendations as currently drafted appear to place the burden on an individual's ability to prove the defence, rather than the onus and burden being on the prosecution to prove the offence (as is the case with the majority of criminal law offences). To the extent that there are defences or exemptions needed, the FTAHK is of the view that these should be available to persons generally, but, as we have provided above, with a focus on the intention and purpose of the individual at the time of commission of the alleged offence.

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

Yes, the FTAHK believes that any defence or exemption should be extended to non-security professionals. As we have set out in our answers to (a) above, the concept of bug bounty programs is prevalent within the IT industry and participants in these programs range from cybersecurity hobbyists to cybersecurity professionals. We also wish to draw the LRC's attention to the increase in open-source software, which by its very nature allows users to use, study, modify and enhance[9]. Users of this software may include non-security professionals and, similarly to bug bounty hunters, those who identify issues and seek to modify/ enhance the software will be acting with an intent to better the community. Requiring accreditation may serve to limit participation from keen hobbyists, thereby

[9] https://opensource.com/resources/what-open-source

limiting the ability to leverage crowdsourcing as a means of identifying potential cybersecurity threats.

The FTAHK does recognise that there is scope for malfeasance and that the increased integration of IT, computers and the internet by the general populace has increased the risk of vulnerability to cybercrimes. However, we are of the view that with reasonable protocols, these risks can be appropriately managed and still allow for the further growth and development of the industry.

## C.2 Illegal Interception of Computer Data

**Recommendation 5:**

(a) Should there be a specific defence or exemption for professionals 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)?

The FTAHK is of the view that the intent behind these activities should be considered when analysing whether any criminal offence has, in fact, taken place.

As a general principle, the FTAHK is of the view that data that is intercepted should be used with the intention to identify and detect potential malicious activity/ attacks and/or malicious behaviour of individuals.

Against this background, the FTAHK believes that there should be a specific exemption for professionals who have to intercept and use the data intercepted in the course of their ordinary and legitimate business, and that any such exemption should exist for not only the network owner, but also their delegated agents and any contracted service providers. We note that interception of computer data is an essential task in the diagnosis of network issues, for example, in acts as innocuous as measuring signal strength, through to testing network security.

However, we believe that such a defence or exemption may be difficult to implement in practice, given the difficulties in crafting a list that will capture all potential legitimate interception and use cases. In addition, the use of the phrase “have to intercept and use” suggests a level of obligation may not necessarily be applicable in all cases.

We would appreciate if the LRC could clarify whether the exemption proposed in this recommendation is only to those who have received prior authorisation to intercept/ use data, or if an individual would be able to claim legitimate business need as the basis of a defence to any alleged offence. We are of the view that in respect of this Recommendation 5, the LRC adopt flexibility in its position as our belief is that the IT industry at present lacks the infrastructure to catalogue all individuals who may have to intercept and use any data so intercepted in the course of their ordinary

and legitimate business activities. As such, flexibility to allow for a combination of exemption and/or defence is preferred.

As a final matter, it is unclear from the Consultation Paper as to whether the LRC has considered the various forms that a network may take and would like to draw the LRC's attention to the nature of mesh Wi-Fi: by its design, mesh Wi-Fi allows for the legitimate re-propagation of transmissions. It should not be the case that individuals operating a mesh Wi-Fi system fall within the scope of any legislation and proposed defence/ exemption.

(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)?

The FTAHK does not consider the examples provided as constituting offences under the proposed language by the LRC. The FTAHK notes that the provision of Wi-Fi services for free in exchange for customer and network data is ubiquitous and a part of everyday life for most netizens.

We are of the view that there are two issues for consideration: (i) authorised collection; and (ii) authorised use.

In the examples provided above (and other uses in the same vein), where customers or employees are required to accept terms and conditions governing the collection and use of data, this would constitute authorised collection.

However, we note that there may be an issue where a genuine business provides Wi-Fi services or a computer to its customers with no terms and conditions governing the collection and use of any customer data. Whilst network owners should have the right to intercept traffic on their own networks, for example, to block/ admit a particular device from a network, this right should be balanced against relevant legal obligations. Here, where there has been no user consent to the collection of data, we note that an offence under the Personal Data (Privacy) Ordinance may have been committed, depending on what data has been intercepted and the extent of personal identifiable information that is contained therein. Were the LRC to legislate around this type of data interception and/or use, the FTAHK would recommend that the proposed legislation around cybercrimes not be duplicative as there is already legislation to address this type of data interception and/or use.

On authorised use: as stated throughout this response, the FTAHK believes that the intention behind the interception and collection of customer data should be taken into consideration when determining whether an offence has been committed: where the basis for interception and collection are legitimate, appropriate defences and/or exemptions should be built into any future legislation. Where data is being intercepted and/or collected for illegal purposes, then such acts should fall within the purview of any proposed legislation. Adopting this mind-frame would

obviate the need for a pre-defined list of legitimate businesses, and given the fast-developing pace of technology, remove the burden of continually updating any such lists.

## C.3 Illegal Interference of Computer System

**Recommendation 8:**

(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?

The FTAHK is of the view that the intent behind these activities should be considered when analysing whether any criminal offence has, in fact, taken place.

If intent is not considered a condition, then the FTAHK is of the view that scanning (or similar forms of testing) of computer systems to evaluate potential security vulnerabilities should be a lawful excuse for the proposed offence of illegal interference of a computer system. As we have noted above, there are instances (bug-bounties, open-source software use) where the act of scanning or any similar forms of testing is not known to system owners at the time of action – whilst one may argue that there is implied authorisation, the recommendations in their current form do not differentiate between implied and express consent.

(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); 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?

The FTAHK repeats its position as set out in the preceding paragraphs – in order to determine whether a criminal offence has been committed, one should look at the *mens rea* of the alleged proponent at the time of the act. The intent behind the act is key.

We note that taking an objective look at the skills referenced within the Consultation Paper, there does not appear to be any real distinction between capable software practitioners and cybersecurity professionals: network security is an in-built facet of every IT professional's job, including database, system, and network administrators, and we note that the development of secure systems by developers, emergence of more integrated development security and operations teams and/or the shift to fully automated administration of systems, databases and networks also blurs the line between who falls under purview of the proposed legislation and who would fall out.

It is worth noting that Denmark, as an example, has introduced the concept of digital self-defence, namely, the use of tools and technologies to protect netizens from an actual or possible cyberattack[10] and is of the view that these means of self-protection should be considered in any future legislation on the issue of cybercrimes.

## C.4 Illegal Interception of Computer Data

**Recommendation 10:**

(a) Should there 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?

The FTAHK is of the view that criminalising these acts may be difficult to effect in practice as there may, in fact, be legitimate basis for the possession of code with the capabilities of scanning, deleting, encrypting, messaging, transmitting, etc. As stated above, we believe that the intent behind the possession or distribution should be considered when analysing whether any offence has, in fact, taken place.

As an alternative to the recommendation, the FTAHK proposes that the LRC consider institutionalising an updateable system to enable the criminalising of certain named software (for example, code that has been identified by malware). This, together with a finding of an intent to harm, would, we believe, serve as a more practical means of criminalising this activity.

(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?

[10] See as an example, the approach taken in Denmark to protect a wide array of societal actors from the threat of cyber-attacks: https://eucpn.org/document/the-danes-digital-self-defense

As stated above, we believe that the intent behind the possession or distribution should be considered when analysing whether any criminal offence has, in fact, taken place.