Submission of the Office of the Privacy Commissioner for Personal Data in response to the Consultation Paper on Cyber-dependent Crimes and Jurisdictional Issues

This submission is made in response to the Consultation Paper on Cyber-dependent Crimes and Jurisdictional Issues ("**Consultation Paper**") published by the Sub-committee on Cybercrime of the Law Reform Commission ("**Sub-committee**") in June 2022.

General Position

2. The Office of the Privacy Commissioner for Personal Data ("**PCPD**") welcomes the proposed bespoke cybercrimes legislation. In recent years, leakage of personal data on the internet has become an unprecedented risk to users and surfers, with the number of data breaches on a steady rise, and such trend has been observed from the data breach incidents handled by PCPD. It is worth noting that cyberattack incidents including ransomware attacks comprised around a quarter of the reported data breaches in recent years: In 2021, the percentage increased to 29% and over 600,000 Hong Kong citizens were affected in various cybersecurity incidents. We consider that the proposed offences would help the government to combat cybercrimes in a more effective manner while incentivising responsible entities to adopt more stringent measures for the protection of cybersecurity. More recently, in response to the increasing threat to cybersecurity, PCPD published a guidance note on data security measures for information and communications technology[1] in August 2022.

[1] Full Guidance Note available at: https://www.pcpd.org.hk//english/resources_centre/publications/files/guidance_datasecurity_e.pdf

Security of Personal Data and PCPD's Data Breach Notification Mechanism

3. It is observed that in the 5 proposed offences, 4 of them directly addressed possible breaches of data security, namely "illegal access to programme or data in a computer" ("**1st Proposed Offence**"), "unauthorised interception of computer data carried out for a dishonest or criminal purpose" (**"the 2nd Proposed Offence"**), "illegal interference of computer data" ("**3rd Proposed Offence**") and "illegal interference of computer system" ("**4th Proposed Offence**"). We support that the creation of the above offences will help to deter data security breach, which has become increasingly common according to our enforcement experience. It is worth nothing that under Data Protection Principle 4 ("**DPP4**") of Schedule 1 of the Personal Data (Privacy) Ordinance Cap. 486 ("**PDPO**"), data user holding any personal data (including data in a form in which access to or processing of the data is not practicable) should take all practicable steps to ensure such personal data is protected against unauthorised or accidental access, processing, erasure, loss or use. Data users who suffer from a data breach incident involving leakage of personal data have been strongly advised to submit a data breach notification to the PCPD and inform the affected individuals early for the proper handling of such incident. Should the abovesaid proposed offences be enacted in the future, the data breach notification mechanism under the PDPO would help identify the breaches and PCPD may refer the cases to suitable law enforcement agency(ies) for further investigation.

Illegal Access to program or data

4. In the Consultation Paper, the 1st Proposed Offence is recommended to "*address dangerous threats to, and attacks against, the security of computer systems*"[2], with hacking listed as one of the examples against which the proposed offence aims to combat. In this context, you may be aware that law enforcement

[2] Paragraph 2.1 of the Consultation Paper

agencies, PCPD included[3], were vested with the power to access suspect's mobile phones for criminal investigation purpose with or without search warrant (under limited circumstances) as authorised by law. Given that the words "illegal" and "unauthorised"[4] would be adopted for the 1st Proposed Offence, we believe that any legitimate access conducted by law enforcement agencies would not fall under the 1st Proposed Offence or would be exempted therefrom.

Illegal interception of computer data for a dishonest or criminal purpose

5. In the Consultation Paper, the 2nd Proposed Offence is recommended to outlaw interception of computer data that is analogous to traditional tapping and recording of telephone conversations not carried out pursuant to legal authority, with the purpose of protecting people's right to privacy of data communication[5]. In particular, unauthorised *disclosure* or *use* of the intercepted data are recommended to be prohibited as well[6]. The 2nd Proposed Offence is recommended to apply to data generally, including metadata[7]. It is also proposed that an offender should be liable to imprisonment for two years on summary conviction and 14 years on conviction on indictment[8].

6. Insofar as the disclosure of personal data with a criminal intent is concerned, we wish to draw your attention, in particular, to the provisions of section 64(3A) and (3C) of the PDPO, namely, two criminal offences under a two-tier structure to curb doxxing:-

[3] Under s.66G(3) of the Personal Data (Privacy) Ordinance Cap. 486, the Privacy Commissioner or any prescribed officer could apply for search warrant to access the electronic device; s.66G(8) further provides that the Privacy Commissioner or any prescribed officer could access the electronic device without search warrant under limited circumstance.
[4] Recommendation 1 of the Consultation Paper
[5] Paragraph 3.1 of the Consultation Paper
[6] Paragraph 3.94 of the Consultation Paper
[7] Paragraphs 3.104 – 3.107 of the Consultation Paper
[8] Paragraphs 7.82 – 7.88 of the Consultation Paper

a. The first-tier offence (section 64(3A) of the PDPO) is a summary offence for disclosing any personal data of a data subject without the relevant consent of the data subject, and the discloser has an intent to or is being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject. Any person who commits the first tier doxxing offence is liable on summary conviction to a fine of HK$100,000 and to imprisonment for 2 years;

b. The second tier offence is an indictable offence for disclosing any personal data of a data subject without the relevant consent of the data subject; where the discloser has an intent to or is being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject; and the disclosure causes any specified harm to the data subject or any family member of the data subject. Any person who commits the second tier doxxing offence is liable on conviction on indictment to a fine of HK$1,000,000 and to imprisonment for 5 years.

7. Furthermore, under section 64(1) of the PDPO, a person commits an offence if he discloses any personal data of a data subject obtained from a data user without the data user's consent with the intention to either obtain monetary gain or other property, whether for his own benefit or that of another person; or to cause monetary loss or other property to the data subject. Any person who commits the offence is liable on conviction to a fine of HK$1,000,000 and to imprisonment for 5 years.

8. Despite the fact that there are apparent differences between the *mens rea* required for the 2nd Proposed Offence[9] and that for the doxxing offences[10], which is relatively specific and confined in scope, and for the section 64(1) offence[11], it appears that, depending on the facts and evidence of the case, the relevant disclosure of personal data may constitute the 2nd Proposed Offence and an offence under the PDPO at the same time.

9. That said, we support the introduction of a new offence of unauthorised interception, disclosure or use of computer data (including personal data) carried out for a dishonest or criminal purpose if the policy intent is to protect people's right to privacy of data communication. We, however, wish to point out that the disclosure or use of computer data (including personal data) apparently constitutes different criminal act separate and distinct from the act of interception. Insofar as the policy intent is to outlaw the disclosure or use of computer data obtained as a result of the prior interception act, we suggest that be spelt out clearly in the legislation. Otherwise, the purview of the new offence may cover the disclosure or use of computer data which are not obtained from the interception.

10. In this context, the Sub-committee may also wish to note that the use (including disclosure or transfer) of personal data is governed by Data Protection Principle 3 ("**DPP3**") of Schedule 1 of the PDPO, and contravention of DPP3 is currently not a criminal offence under the PDPO.

11. As regards the question of whether there should be a defence or exemption for professions who have to intercept and use the data intercepted in the course

[9] "for a dishonest or criminal purpose"
[10] "intent to or is being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject"
[11] "with the intention to obtain gain in the form of money or other property, whether for his own benefit or that of another person; or to cause loss in the form of money or other property to the data subject."

of their ordinary and legitimate business, we wish to point out that where the collection or use of the data in question concerns personal data, the collection and use may, depending on circumstances, be regulated by DPP1 and DPP3 respectively under the PDPO. In particular, DPP3 provides that "personal data shall not, without the prescribed consent of the data subject, be used for a new purpose [other than the purpose for which the data was to be used at the time of the collection of the data or a directly related purpose]".

Response to Recommendation 5 of the Consultation Paper

12. The Sub-committee has invited submission on whether a genuine business 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. As rightly pointed out by the Sub-committee in paragraph 3.118 of the Consultation Paper, the authority to intercept and utilise the data in such scenarios is often contractual in nature. We have reservations on whether criminal liability should be imposed in such scenario as the relevant customers or employees are usually explicitly/ implicitly informed of, and agree to, the collection of data. Again, where the collection concerns personal data, such collection and use of personal data are governed by the DPPs under the PDPO.

Response to Recommendation 8 of the Consultation Paper – Data Scraping

13. In the Consultation Paper, the 4th Proposed Offence has been suggested to "*prohibit hinderance of lawful use of computer systems by using or interfering with computer data, and thereby protecting the proper functioning of computer system*"[12]. DDOS attack and slow attack have been raised as examples that could be criminalized under this proposed offence. The Sub-committee invites submissions on whether there should be lawful excuse to the proposed offence of

[12] Paragraph 5.1 of the Consultation Paper

illegal interference of computer system for non-security professionals, such as web scraping and unauthorised scanning of a service provider's system (cf. paragraph (b) of Recommendation 8). In this context, it appears to us that "web scraping" may include “data scraping”, where a computer programme extracts data from human-readable output produced by another programme. In PCPD’s enforcement experience, the personal data collected by data scraping would sometimes be sold in the dark web without the knowledge and consent of the data subject, with the scrapping itself constituting a data breach incident. To enhance cybersecurity, in our view unauthorised web scraping (including data scraping) and scanning of a service provider's system should also be caught by the proposed offence, and only consensual, or lawful, interference of computer system should constitute a defence to the offence.

Response to Recommendations 11 – 15 of the Consultation Paper

I. Extra-territorial effect

14. PCPD supports the extra-territorial application of 1st – 4th Proposed Offences. In our enforcement experience, given the borderless nature of the internet, it is very common that the perpetrator is not a Hong Kong person or does not reside in Hong Kong at the time the crime is committed, and thus has no connection with Hong Kong at all. We therefore support the Sub-committee’s recommendation against including fact pattern (b) in paragraph 7.69 of the Consultation Paper i.e. the perpetrator being a “Hong Kong person”.

15. Furthermore, we observe from our enforcement experience that often the target computer, program or data, albeit storing the personal data of Hong Kong persons, is not located in Hong Kong. In the premises, in order to ensure the effectiveness of combatting cybercrimes, we suggest removing the requirement stipulated in (c) of Recommendations 11 – 14.

16. We also note that the concept of "Hong Kong person" under the Proposed Offences is recommended to include "*Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong*"[13]. We invite the Sub-committee to refer to section 66M(5) of the PDPO regarding the cessation notice mechanism in respect of doxxing messages, where a "Hong Kong person" is defined as *"(a) an individual who is present in Hong Kong; or (b) a body of persons that – (i) is incorporated, established or registered in Hong Kong; or (ii) has a place of business in Hong Kong*". We believe that the formulation is more straight-forward, simpler and has less room for argument than one using the more complicated formulations of permanent residency or ordinary residence, as complicated factual and legal questions often arise as to what constitutes "permanent residency" or "ordinarily" residing in a particular place.

II. ***Critical Information Infrastructure***

17. It is noted that for all Proposed Offences, Hong Kong courts is recommended to have jurisdiction where *"(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*". In this context, we would like to invite the Sub-committee to note the notion of "Critical Information Infrastructure" ("**CII**") adopted in the *Cybersecurity Law* of the PRC, as further elaborated under the *Rules on the Protection of the Security for Critical Information Infrastructure* recently promulgated. In addition, the proposed cybercrimes legislation may also need to take into account the provisions and approach of the cybersecurity law which is under deliberation by

[13] Footnote 80 of the Consultation Paper

the government, bearing in mind that CII may be one of the areas of protection under that law.

Dated this 19th day of October 2022.

(Billy Kwan)
Assistant Privacy Commissioner for Personal Data (Acting)
(Complaints and Criminal Investigation)
for The Privacy Commissioner for Personal Data, Hong Kong