Asia Internet Coalition (AIC) Industry Representation on

Hong Kong Personal Data (Privacy) (Amendment) Bill 2021

12 August 2021

To
The Bills Committee
Personal Data (Privacy) (Amendment) Bill 2021
Legislative Council Secretariat
Legislative Council Complex, 1 Legislative Council Road
Central, Hong Kong

Subject: Industry Comments on Hong Kong Personal Data (Privacy) (Amendment) Bill 2021

On behalf of the Asia Internet Coalition (AIC) and its members, I am writing to express our sincere gratitude to the Constitutional and Mainland Affairs Bureau (**the Bureau)**, **the Bills Committee**, and the **Office of the Privacy Commissioner for Personal Data (PCPD)** to submit comments on the **Personal Data (Privacy) (Amendment) Bill 2021**. AIC is an industry association of leading Internet and technology companies in the Asia Pacific region with an objective to promote the understanding and resolution of Internet and ICT policy issues.

First and foremost, I would like to express our sincere gratitude to PCPD for the opportunity to virtually meet to discuss the proposed amendments to Hong Kong's Personal Data (Privacy) Ordinance on 9 July 2021. Indeed, the meeting provided us with important insights on the Office of the Privacy Commissioner for Personal Data (PCPD)'s objectives for the legislative amendments. We also appreciate the PCPD's invitation for AIC to submit further comments once the Amendment Bill has been published.

The AIC wishes to reiterate that doxxing is a matter of serious concern, a view that AIC shares with Hong Kong. We also appreciate the importance of privacy and the protection of personal information and are therefore committed to the principles that safeguard users' personal identities. To this extent, the AIC and its members are strongly committed to continue working together with the PCPD to develop effective policies to support Hong Kong's continued digital growth and transformation. As such, please find appended to this letter, **detailed comments and recommendations** which we would like to respectfully request the PCPD and the Bills Committee to consider.

We are also currently in the process of drafting the **Proposed Language Changes to Hong Kong Personal Data (Privacy) (Amendment) Bill 2021**, which will be submitted to the Bills Committee and PCPD in due course.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact us at the Secretariat, Mr. Sarthak Luthra (Secretariat@aicasia.org). Furthermore, we look forward to further discuss our comments and recommendations in order to shape the dialogue for the advancement of data protection in Hong Kong.

Once again, thank you very much for this opportunity.

Sincerely,

Jeff Paine

Managing Director
Asia Internet Coalition (AIC)

Detailed Comments and Recommendations

---

1. Scope of the Doxxing Offence

Given the criminal nature of the two offences under Section 64(3A) and 64(3C), in particular where a criminal offence may be committed by an act of disclosure of personal data even though specified harm has not actually been caused to the data subject or a family member of the data subject under Section 64(3A), we consider that the scope of the offences are too broad and should be made more specific. In particular:

- It bears repeating that the Legislative Council Panel on Constitutional Affairs proposed the doxxing offence specifically to combat doxxing acts "*which intrude into personal data privacy.*" Such acts were described in its 17 May 2021 Discussion Paper as those which "*in effect weaponise personal data*", and which "*have caused great harm to the victims*". The omission of any requirement for actual harm to be proved not only departs from this intent, but also introduces significant risks of excessive and/or overbroad application of the offence and creates an opaque operating environment for platform service providers and citizens alike. Apart from a subjective requirement relating to intention, there is nothing else in the language of the offence that would clearly prevent it from being used as a tool for censorship, or be otherwise misused to criminalize everyday activities involving harmless disclosure of another person's personal data (e.g., mentioning a name or posting a photo online). The doxxing offence should be harm-based with a high threshold to prevent opening up a floodgate of doxxing cases,

and to retain the original intent of the amendment by directly addressing the harm caused to doxxing victims.

- Given a specific harm does not have to crystallise, as long as there is intent or recklessness toward causing such harm, the evidentiary threshold is unclear. It appears for a first tier doxxing offence to have occurred, there is no requirement for proof of any actual specified harm. This creates an unclear enforcement environment for platform service operators.

- Further, the phrase "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" as currently drafted does not require a proof of intent. As a comparison, "recklessness" would not be a sufficient proof of intent under Section 24 of the Crimes Ordinance in relation to certain acts of intimidation prohibited. We propose specifying that it is necessary to prove an intent in addition to "recklessness".

- "Family member" refers to a person "who is related to the person by blood, marriage, adoption or affinity" as currently drafted. The scope of family members related by "blood" or "affinity" is too vague and broad under the offence under Section 64(3A) where no actual specified harm is actually caused to the family member. We propose narrowing down the definition of "family member" to bring more certainty and specificity in the context of criminal offences. Consideration should be given to restricting "family members" to persons related by marriage, filiation or adoption for the purpose of the doxxing offence.

- We would also like to seek clarification in Section 64(3A) if "discloses" may cover disclosure to public or in private communications. It is not clear if the law is applicable only to public user generated content, or whether it might also apply to private communication.

- The proposed definition of "Specified Harm" includes "pestering", "threat", "harm causing a person reasonably concerned for his/her well-being" without any degree of seriousness being attached. This definition is not specific and objective enough for a criminal offence punishable up to 5 years of imprisonment on indictment. It is important to note that the current proposed offence involves a disclosure of personal data about a data subject without consent as opposed to criminal offences relating to harassment or causing bodily harm, or damage to property. Additional factors should be taken into consideration when considering the level of harm to qualify as "specified harm", for example:

    - *cf* "harm to an ordinary reasonable person in the position of the victim" under New Zealand's Harmful Digital Communications Act (HDCA) which also lists out relevant factors to be taken into account when considering whether a digital post would cause "harm";

- actual threats of a serious nature e.g. threat to kill, threat to cause serious harm, or actual conduct that "reasonable persons regard in all circumstances as menacing, harassing or offensive" under Australia's Criminal Code Act 1995;
- conduct that causes another person to "reasonably, in all the circumstances, to fear for their safety", and "prohibited conduct" comprise of "repeated communications" or engaging in threatening conduct directed at other persons or member of their family under Canada's Criminal Code;
- "putting people in fear of violence" in the UK i.e. conduct that causes another to fear, on at least two occasions, that violence will be used against another, if the person knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

- We propose that the definition of "specified harm" under Section 64(6) should be carefully revisited and revised to remove acts which are not in themselves criminal in nature e.g. pestering or intimidation (as opposed to criminal intimidation). The reference to "threat" should be narrowed to threats to cause death or bodily harm, or damage to property, but not generally to any threat.

- Further, the definition of “specified harm” includes “psychological harm”. Given that interpretation of the term “psychological harm” is highly discretionary, can potentially be very broad and does not provide an objective standard for application, we seek clarification on how “psychological harm” will be construed and established under the proposed doxxing offence.

- We also seek clarification on what evidence will be provided of “specified harm” having been incurred, and what evidence will be provided of a person’s recklessness that “specified harm” may occur.

- Under Section 64(4)(d)(i), the current drafting suggests that “for the purpose of a news activity” will be revised to “solely for the purpose of a lawful news activity”. We seek clarification on the reason for adding “solely” and “lawful”.

- We propose a broader public interest / data subject and family member interest defence, considering the significant expansion of scope of the doxxing offence. The current “public interest” defence linked to “lawful news activity” may not cover situations where there is reasonable ground to believe that the disclosure was for public interest or the interest of the data subject and/or family members outside the scope of news activity. Reference can be made to Singapore's Protection from Harassment Act 2014, which provides that, in relation to the crime of publishing any identity information of a target person or a related person of a target person with a result causing the target person or other person harassment, alarm or distress, it is a defence to prove that the conduct was reasonable.

We note that subjecting intermediaries and their local subsidiaries to criminal investigations and prosecution for doxxing offences under the proposed amendments is a serious penalty,

given that intermediaries are neutral platforms with no editorial control over the doxxing posts, and are not the persons making the posts. Penalizing platforms for their users' doxxing actions, over which platforms have no control, is a very extreme outcome and we request further clarity on procedural elements impacting platforms.

2. Intermediary Liability

The proposed amendments empower the PCPD to serve a cessation notice on any person for rectification actions, to be taken within a designated time frame, when it has the grounds to believe that there is a breach of Section 64 of the PDPO.

- We noted that Section 66M (service of cessation notice) can apply extraterritorially. We seek clarity on that proposal and especially the legal basis of enforcing extraterritorial provisions against foreign entities. Under section 66M, a cessation notice may be served on a "Hong Kong person", which includes a company which "has a place of business in Hong Kong". We seek clarity in the drafting language that the notices will be served on non-Hong Kong service operators and not their local affiliates. We emphasise that not all international intermediaries operate their services from within Hong Kong, and local representatives or sales offices located in Hong Kong are not the appropriate recipients for notices under the proposed amendments. As modes of service are not articulated in the proposed amendments, we also seek clarity on the intended modalities for extra-territorial service.

- Section 66N contemplates that there will be an appeal mechanism for the cessation notice, and Section 66N requires a cessation notice to be complied with within the stipulated time frame pending the outcome of any appeal to the Administrative Appeal Board (AAB), and failure to do so could expose intermediaries and employees to criminal prosecution.

    - As stated in our submission dated 25 June 2021, it is not uncommon for the AAB to take a very long time to hand down a decision under the appeal mechanism. We reiterate our proposal of specifying a reasonably prompt deadline for the AAB to provide an appeal decision in order to balance the interests between the victims of doxxing activities and the public's rights to access information.

    - Further, the proposed regulation requiring compliance with a cessation notice pending the outcome of the appeal is disproportionate and unnecessary. It is our experience that most intermediaries already have a notice and takedown regime in place to deal with doxxing content and such requests would be responded to without undue delay.

3. <u>PCPD's Enforcement Power</u>

Section 66D empowers the Privacy Commissioner to require a person (which can be a corporate entity) to provide information, materials and assistance. We consider that the proposed powers of the Privacy Commissioner are overly broad, and there is a lack of judicial guidance on how Section 66D may operate in practice. The provisions under Section 66 D, E and H are concerning, which allows the Commissioner with unprecedented powers to search and arrest a person without warrant. Therefore, we recommend that the Bill limits the definition of "person" to the individual posting the information, or at maximum, the corporate entity storing or hosting the information.

In particular:

- Section 66D(2)(d) & (e) empowers the Commissioner to require a person "to make a statement" and/or to "give all the assistance the Commissioner reasonably requires". Similar to the above, we consider that the powers are overly broad and disproportionate in the context of data protection.

- The use of the term "reasonably *suspects*" in Section 66D(1) followed by the use of terms "reasonably *believes to* be relevant" and "reasonably *requires*" in Section 66D(2) introduce inconsistent standards which the Commissioner is expected to adopt when Sections 66D(1) and 66D(2) deal with the same subject matter. As noted above, there is currently no judicial guidance on the interplay of the various standards and thus this creates additional uncertainty. We also seek clarity on what the threshold for reasonableness will be for the purposes of any data disclosure request.

- Section 66E(4) provides that a person is taken to have established a reasonable excuse of not complying with an order from the Commissioner if, amongst other things, he is able to adduce "sufficient evidence" for the reasonable excuse. It is unclear why the proposed amendments cannot introduce what may amount to "sufficient evidence", an approach commonly adopted in other ordinances (e.g. Copyright Ordinance (Cap. 528)).

- Unlike the cessation notice under Sections 66J to O, there is no statutory appeal mechanism against the issuance of a notice made pursuant to Section 66D(2). This means that if a person disagrees with the notice, the only judicial recourse would be to seek a judicial review of the Commissioner's decision. A judicial review action is costly and time consuming. The alternative would be to disregard the notice and wait for potential criminal prosecution, at which time, one can try to raise a reasonable excuse, but it is not generally considered a feasible option for a well-established corporation or its employees to wait to be prosecuted and only raise a defence at that time. Given the wide application of Section 66D, the potential approaches currently contemplated under Section 66E are unsatisfactory.

- Sections 66J to O relating to cessation notice contain some restrictions on how the power may be exercised by the Commissioner (e.g. the content which a cessation notice must contain). However, none of these restrictions are provided for in connection

with an information request/investigation notice issued under Section 66D(2) which could potentially have similar commercial ramification for corporations, i.e. legal obligations owed to its customers and business partners may be compromised, if a corporation chooses to comply with the notice. We seek clarification as to why a different approach is adopted for such notice.

- Section 66G(8)(c), 66H allows an authorized officer to have the broad power to stop, search, arrest, and access electronic devices without warrant akin to that of a police officer. Also, Section 66H(3)(b) empowers an authorized officer to search and take possession of anything from an arrested person which the officer reasonably suspects "may throw light on the character or activities of the person". This provides wide power to an authorized officer to seize personal items of an arrested person based on vague grounds and without the need to establish a reasonable degree of relevance between the item and the unlawful act being investigated. We consider that the broad scope of the proposed power is not justified in the context of data protection laws and may cause disproportionate impact on individuals and corporations. In particular, we would like to further understand the necessity and relevance of empowering an authorized officer to search and take possession of anything from an arrested person which the officer reasonably suspects "may throw light on the character or activities of the person" in the context of a doxxing offence.

- Further, the Commissioner's powers in relation to premises and electronic devices are circumscribed by Section 66G. However, sub-sections relating to the exercise of these powers can benefit from a greater degree of clarity.

    - First, we note that the requirement for a magistrate's warrant is subject to Section 66G(8), where the Commissioner or any prescribed officer may "*without warrant, access the device*" if an application for a warrant is "*likely to defeat the purpose of accessing the device, or for any reason it is not reasonably practicable to make the application*." The ability to sidestep the requirement for a magistrate's warrant is significant, and we seek further clarity on examples where Section 66G(8) will be used.

    - Second, Section 66G(6) states that "*a specified person must, without charge, afford facilities and assistance reasonably required by the Commissioner or any prescribed officer for the purposes of the specified investigation*." As previously noted, this would include intermediaries, their local subsidiaries and personnel and is a disproportionate measure for intermediaries who are not the primary author of doxxing content. We again reiterate that intermediaries, their local subsidiaries and staff be excluded from the scope of this section.

    - As Section 66G(3)(c) expressly recognises decryption of material as a power that may be exercised in relation to an electronic device, we seek clarity on whether the Commissioner may compel a specified person (e.g., an employee of an international intermediary) to provide technical assistance to decrypt

information (e.g., build a backdoor or bypass encryption) on threat of violating Section 66I. This would be relevant where, for example, such materials are stored in end-to-end encrypted applications or cloud backups.

4. Secrecy

Section 66Q imposes secrecy requirements on four categories of persons (defined as "persons concerned"), including "a person assisting the Commissioner or a prescribed officer". We seek clarification on whether "a person assisting the Commissioner" includes a person being required by the Commissioner to provide information and assistance under Section 66D. Arguably, a person required by law to do certain things can only be said to be complying with obligations when doing the thing required of him/her, and would not ordinarily be said to be "performing his/her function". Also, the definition of "persons concerned" does not include a person arrested or being subject to investigation under the offence so on this basis, we consider that Section 66Q as currently drafted should only be interpreted to cover persons from the law enforcement side. If the provision does intend to cover those arrested, being investigated or required to provide assistance, we propose adding an exemption for disclosure to obtain legal advice, which is not currently built in.