25 June 2021

Ms Ada Chung Lai-ling
The Privacy Commissioner for Personal Data
Office of the Privacy Commissioner for Personal Data (PCPD), Hong Kong

Subject: Industry Response on the Proposed Amendments to Hong Kong's Personal Data (Privacy) Ordinance and Request for Virtual Meeting with PCPD

Dear Ms Ada Chung Lai-ling,

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)** and the **Office of the Privacy Commissioner for Personal Data (PCPD)** to submit comments on the **Amendments to the Personal Data (Privacy) Ordinance (PDPO)**. As an introduction, 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. AIC has submitted several policy positions to the key agencies in the Government including PCPD in Hong Kong.

The AIC understands that the Amendments to the Privacy Ordinance particularly focus on safety and personal data privacy of individuals. However, we wish to stress that doxxing is a matter of serious concern and is a view that the AIC shares. As responsible stakeholders in this policy formulation process, we would greatly appreciate the opportunity to share our comments on these proposed amendments. As such, please find appended to this letter, detailed comments and recommendations which we would like to respectfully request the PCPD and the Bureau to consider when reviewing the Amendments to the Privacy Ordinance.

We appreciate that the **Office of the Privacy Commissioner for Personal Data (PCPD),** recognises the importance of public-private dialogue to co-create policies for a better digital future of Hong Kong. The AIC stands strongly committed to working together with PCPD and aims to play an active role in steering the data protection framework in Hong Kong. **Based on this response submitted, we would also like to request for a video conference meeting with you or your team, if your time allows, to further discuss the proposed amendments and elaborate on our submission.**

Please accept, the Commissioner, the assurances of our highest consideration. Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490.

Thank you

Sincerely,
Jeff Paine
Managing Director, Asia Internet Coalition (AIC**)**

Cc: Mr Erick Tsang Kwok-wai,
Secretary for Constitutional and Mainland Affairs Bureau,
12/F, East Wing, Central Government Offices, 2 Tim Mei Avenue, Tamar, Hong Kong

Detailed Comments and Recommendations

Doxxing is a matter of serious concern, a view that AIC shares with the Panel on Constitutional Affairs' (the "Panel"). 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 through community standards on privacy violations

We also believe that any anti-doxxing legislation, which can have the effect of curtailing free expression, must be built upon principles of necessity and proportionality.

As such, we welcome the opportunity to provide our comments on how amendments to Hong Kong's Personal Data (Privacy) Ordinance ("PDPO") could be further developed in line with international principles and norms.

1. **Definitions of doxxing**

   The stated purpose of the proposed amendments to Hong Kong's Personal Data (Privacy) Ordinance ("PDPO") is to introduce anti-doxxing laws to "*combat doxxing acts which intrude into personal data privacy*". Notwithstanding this, the paper setting out the proposed amendments to the PDPO did not provide a definition for the term "*doxxing acts*", and merely described doxxing acts to be actions that are "*intrusive to personal data privacy and in effect weaponise personal data*".

   The definition of "*doxxing acts*" in the proposed amendments creates problematic ambiguity - in particular, given that at present there is no universally accepted or acknowledged definition for "*doxxing*", this gives rise to legitimate concerns that "*doxxing*" in the proposed amendments could have an overly broad interpretation such that even innocent acts of sharing of information online could be deemed unlawful under the PDPO.

   The scope of any restrictions on content and free expression should be clearly defined so that both intermediaries and users can better understand the aim, impact, and application of these regulations, as well as to avoid any inadvertent or unintended violations. By keeping the scope of the restrictions vague, significant discretionary authority lies with regulators to restrict content, while also making it difficult for intermediaries to put systems in place to handle any such "inappropriate" content in a practical and scalable manner.

   The proposed doxxing offence to be added to Section 64 of the PDPO requires that the disclosed information of the data subject will either "threaten, intimidate or harass" or cause "psychological harm" when disclosed without the data subject's consent.

Our view is that "psychological harm" should not be part of the test for conviction under the proposed doxxing offence, 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 therefore ask that the PCPD remove "psychological harm" from the proposed doxxing offence.

In the alternative, we seek PCPD's clarification on how "psychological harm" will be construed and established under the proposed doxxing offence.

2. Adding doxxing as a new offence

The proposed anti-doxxing provision does not take into account legitimate situations where personal data may be disclosed without the data subject's consent. For example, the drafting does not exclude situations where information (including personal data) is disclosed by a person to establish/defend his or her legal rights, or where there is a public interest to know. This doxxing provision may also be triggered where for example a person exposes an incident to the media that contains personal data.

Recommendation

We propose having carve-outs to cater for legitimate situations where personal data may be disclosed without the data subject's consent. Consideration could be given to explicitly bringing in the Exemptions section under the Personal Data Protection Ordinance (PDPO) and have those constitute exceptions under this proposed offence; further or alternatively, add "without lawful excuse" as a qualifier to the offence (Section 50B of the PDPO provides a similar approach).

The current proposal seems to indicate that searching, aggregating, consolidating and re-publishing personal information which is already available in the public domain (assuming that no use restrictions have been set) will constitute a doxxing offence with no exemptions. Therefore, adequate exemptions should be put in place to balance the need to curb doxxing activities and the need to maintain a free flow of information for legitimate purposes.

3. Statutory framework and appropriate regulator

The PDPO is not the appropriate statutory instrument, and the PCPD is not the appropriate regulator, for doxxing-related offences

It is important to note that doxxing is distinct from privacy and personal data issues. We welcome further industry consultation on this important issue. While acts of doxxing necessarily involve personal data, it does not immediately follow that the PDPO is the appropriate statutory instrument for introducing amendments relating to doxxing.

As the Panel noted, Section 64 was "*not intended to address the doxxing acts committed in recent years*", alluding to a broader point that the PDPO itself was not designed to address such issues. The original aims of the PDPO, as contemplated in the 1994 Report on Reform of the Law Relating to the Protection of Personal Data, were to allow Hong Kong to retain its status as an international trading hub through participation in the burgeoning international exchange of personal data, and to give effect to its human rights treaty obligations such as Article 17 of the International Covenant on Civil and Political Rights (ICCPR) instead.

These amendments would irreversibly change the function of the PCPD from what was originally intended. It bears observation that, under Sections 38 and 50 of the PDPO, the PCPD already has powers of investigation and the ability to issue enforcement notices directing data users to remedy and prevent recurring contraventions. Failure to comply with such an enforcement notice is an offence under Section 50A. Introducing these amendments would effectively empower an independent statutory authority to a level akin to the Hong Kong Police Force itself, and in a manner that is highly unusual and out of step with international privacy developments. There are, to our knowledge, no other jurisdictions in Asia-Pacific which have introduced equivalent powers to statutory authorities.

Proposals to further empower the PCPD are not new, and in the Report on Further Public Discussions on Review of the Personal Data (Privacy) Ordinance dated April 2011, proposals to further strengthen the PCPD's criminal investigation and prosecution powers were met with significant opposition. Most respondents considered such powers to be "*excessive*" and likely to "*cause confusion over [the Commissioner's] role and deter data users from seeking help from him to comply with the requirements of the PDPO.*" Even in other well-regarded privacy jurisdictions such as Singapore, powers of investigation accorded to the Privacy Commissioner require inspectors to provide detailed written notice or to successfully apply for a court warrant prior to exercising similar search and seizure powers.

We would welcome further consultation on the benefits of housing anti-doxxing regulation outside the ambit of the Privacy Commissioner. Given the context above, we also seek more clarity on the government's plan to equip the PCPD with the adequate resources and capability to exercise the new enforcement power.

4. Intermediary liability

Exclude overseas-based intermediaries and their subsidiaries from (a) the scope of "persons" and "premises" that are subject to the PCPD's powers to investigate and prosecute; and (b) the scope of "persons" required to first comply with a Rectification Notice pending the outcome of an appeal against the Rectification Notice

The proposed amendments empower the Privacy Commissioner for Personal Data ("PCPD") to carry out extensive criminal investigations on any persons for breach of section 64 of the PDPO,

including making requests for information, documents or things, requiring any person to answer relevant questions to facilitate investigations, and gaining entry into any premise (with the court's permission) and seizing documents or things from the premises as evidence for prosecution proceedings; criminalises any failure to comply with the PCPD's criminal investigations or deliberate attempts to deceive or mislead the PCPD; and empowers the PCPD to initiate prosecution for contravention of Section 64 of the PDPO or failure to comply with the PCPD's requests relating to criminal investigations.

The usage of the terms "*any persons"* and "*any premises*" in the proposed amendments suggests that intermediaries and their local subsidiaries would be within scope for investigation and prosecution under the proposed amendment. We respectfully disagree with this expansive scope.

From an industry standpoint, subjecting intermediaries and their local subsidiaries to criminal investigations and prosecution for doxxing offences under the proposed amendments is a completely disproportionate and unnecessary response to doxxing, given that intermediaries are neutral platforms with no editorial control over the doxxing posts, and are not the persons publishing personal data. What the platforms do is to provide a service / noticeboard to users to post user-generated content. The proposal to subject such platforms to criminal liability is unnecessary and excessive, noting that these platforms are just making the service available to users for posting and should not be penalized for their users' doxxing actions over which the platforms have no control.

We therefore ask that the PCPD exclude intermediaries and their subsidiaries from the scope of "*persons*" and "*premises*" that are subject to the PCPD's powers to investigate and prosecute.

5. Empowering the PCPD to demand the rectification of doxxing content

We ask that the PCPD excludes intermediaries and their subsidiaries from the scope of "persons" required to first comply with a Rectification Notice pending the outcome of an appeal against the Rectification Notice.

We are concerned about the following remarks made at the Legislative Council meeting on May 17, 2021:

- The PCPD or the Administration may prosecute the local staff of overseas platforms in case of failure to comply with the authorities' removal requests.
- If a website or platform consists entirely of doxxing information, the PCPD or the Administration can block these websites from being accessed in Hong Kong.

The proposed amendments empower the PCPD to serve a Rectification 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. This proposed power is intended to have extraterritorial effect, *viz* the PCPD can serve a Rectification Notice to *"... any person who provides in Hong Kong to Hong Kong residents, so as to direct the relevant online platform to rectify the doxxing content".*

The proposed amendments contemplate that while there will be an appeal mechanism for the Rectification Notice, any person being served with the Rectification Notice is required to first comply with the notice within the designated time frame pending the outcome of the appeal, and failure to do so could expose the employees of intermediaries to criminal prosecution.

With respect, the proposed regulation requiring compliance with a Rectification Notice pending appeal the outcome of the appeal is disproportionate and unnecessary.

In reality, most intermediaries already have notice and takedown regimes in place to deal with doxxing content and such requests would be responded to without undue delay.

Recommendation

a. Based on our understanding, for most if not all of the overseas platforms, their online services are provided by their respective offshore global or regional headquarter companies, as opposed to their local subsidiaries in Hong Kong. The local staff of overseas platforms in Hong Kong are not responsible for the operations of the platforms; neither do they (or the local subsidiary by which they are employed) have access right or control to administer the online platform contents.

   Any rectification notice, therefore, may only be legitimately issued against the real operating entity of the online services platform outside of Hong Kong, and it would be a fallacy to issue the same against their local subsidiaries or entities, or to hold them or their employees legally liable for the same.

b. Across aspects of social life, introducing sanctions aimed at individuals is not aligned with global norms and trends, and with tort law generally. It is normally reserved for those persons that actively and wilfully participate and direct activities that evidently cause physical harm. Introducing severe sanctions and especially personal liability in relation to assessing requests for taking down content has the consequence of encouraging online platforms to conduct little to no review of requests and over-block content, which will likely result in grave impact on due process and risks for freedom of expression and communication. The only way to avoid these sanctions for technology companies would be to refrain from investing and offering their services in Hong Kong, thereby depriving Hong Kong businesses and consumers, whilst also creating new barriers to trade. Thus, the possibility of prosecuting subsidiary employees will create uncertainties for businesses and affect Hong Kong's development as an innovation and technology hub. If it remains the PCPD or the Administration's intention to hold the employees of the local subsidiaries or entities liable for doxxing content, we seek clarification on the legal basis of doing so.

c. Last year, the decision of the Administrative Appeals Board (AAB) hearing (X v. Privacy Commissioner) concluded that the extraterritorial jurisdiction of PDPO will not apply to a foreign entity, unless as a data user, it has operations in, or from, Hong Kong, so the rectification notice (if any) should theoretically only apply to the local entities which provide online service in Hong Kong.

d. A free and open internet has been critical for Hong Kong's development as an innovation and technology centre. While we acknowledge the PCPD's goal to reduce the spread of doxxing content, shutting down or blocking the access of websites in their entirety would be a disproportionate response and may create unintended consequences. If it remains the PCPD or the Administration's intention to block access to websites, we seek further clarification on the legal basis and the implementation mechanism of doing so.

e. We note that it is not uncommon for the AAB to take a very long time to hand down a decision under the appeal mechanism. We propose 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.

f. The court has wide inherent jurisdiction to grant injunctions and granted injunctions prohibiting doxxing activities during the social unrest in 2019. To this end, we would like to understand the rationale behind the proposal to empower the PCPD to apply to court for an injunction if he/she is satisfied that there is or it is very likely that there are large-scaled or repeated contraventions.