

# GOVERNMENT PROPOSES NEW CHANGES TO HONG KONG'S DATA PRIVACY LAW TO TACKLE DOXXING

As foreshadowed in the paper prepared by the Hong Kong Government on the proposed reforms in personal data privacy law and submitted to the Legislative Council Panel on Constitutional Affairs for discussions on 20 January 2020<sup>1</sup>, the Government, on 16 July 2021, gazetted its concrete proposals on how the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) should be amended. It came as no surprise that the proposed amendments focus primarily on tackling doxxing and strengthening the powers of the Privacy Commissioner for Personal Data (Commissioner) to investigate and prosecute doxxing-related offences.

It is not debatable that doxxing, which is effectively malicious disclosure of an individual's personal data without his/her consent, is a serious concern which needs to be properly addressed as the current data protection law does not<sup>2</sup>. There are debates, which started even before the Personal Data (Privacy) Amendment Bill 2021 (Bill) was introduced, on how the proposed anti-doxxing law would affect social media platforms, telecommunication carriers and the like. It is therefore worthwhile to take a closer look at the Bill from that perspective.

## Primary offences of doxxing

The Government proposes to criminalise doxxing under a two-tier structure:

*First-tier summary offence* - Anyone who discloses personal data without the data subject's consent, with an intent to cause any specified harm to the data subject or any of his/her family members or being reckless as to whether any specified harm would be, or would likely be, caused, may face a maximum penalty of two years' imprisonment and a fine of HK\$100,000;

<sup>1</sup> For details, please refer to our previous client briefing "[A new year, a new privacy law for Hong Kong?](#)".

<sup>2</sup> Section 64(2) of the existing PDPO contains an offence to protect data subjects against improper disclosure of their personal data which was obtained from a particular data user without the data user's consent and where the disclosure causes psychological

*Second-tier indictable offence* - Anyone who commits the first-tier summary offence may face indictment and more severe penalty if the disclosure in fact causes the specified harm. The maximum penalty is five years' imprisonment and a fine of HK\$1 million.

A key element of the proposed doxxing offences is the disclosure of personal data by the offender, which could be done by way of a post on an online platform. Another key element is "specified harm", whether intended or actually caused, which is given a meaning that is much wider than "psychological harm" contemplated under the current PDPO<sup>3</sup>. The term is proposed to refer to (i) harassment, molestation, pestering, threat or intimidation; (ii) bodily harm or psychological harm; (iii) harm causing a person reasonably to be concerned for his safety or well-being; or (iv) damage to a person's property. Further, the offences extend to cover any specified harm intended to be inflicted on not only the data subject but also people who are related to the data subject by blood, marriage, adoption or affinity.

Therefore, if a person posts information about another person on a social networking site with an intent to hurt the data subject's (or a family member's) feeling or to encourage cyberbullying, he/she will be caught by the proposed anti-doxxing law. He/she may even be convicted on indictment if, as a result of the post, a stranger attacked the data subject or any of his/her family members on the street.

In Hong Kong, an agreement to commit an offence amounts to the crime of conspiracy and the persons involved in the agreement may be prosecuted for the offence. The offence of conspiracy may be charged under section 159A of the Crimes Ordinance (Cap. 200). The Bill makes it clear that the Commissioner may prosecute an offence of conspiracy to commit a doxxing

harm to the data subject. However, the elements for establishing the offence take no account of the consent of the data subjects whose data was being disclosed.

<sup>3</sup> Section 64(2) of the existing PDPO.

offence. Potentially, two or more individuals may be charged with an offence of conspiracy to commit a doxxing offence if they agree with one another that one of them will reveal someone else's private information on an online platform so as to make the data subject or his family member a target of malicious attacks.

A few grounds of defence to the doxxing offences are proposed. A person could be exonerated if, at the time of disclosure, he reasonably believed that the disclosure was necessary for preventing or detecting crime or that the data subject had agreed to the disclosure, or if the disclosure was required or authorised by law or a court order. Currently, a public interest defence is available to those who are engaged in news activities<sup>4</sup>. The Government proposes that the defence will only be available if the person charged can establish that the sole purpose of the disclosure was for a "lawful" news activity.

#### **New power to direct cessation of doxxing activities and contents**

Apart from the prosecution power as mentioned above, the Government proposes that the Commissioner will be empowered to issue notices to remove doxxing contents and even to cease or restrict access to online platforms which contain those contents. This proposal, in particular, has sparked concerns on the part of online and technology firms whose services are currently accessible to the Hong Kong public.

The relevant provisions are summarised as follows:

- (a) The Commissioner may issue a cessation notice if it has reasonable grounds to believe that there is a written message or electronic message whereby personal data has been disclosed without the data subject's consent, and that the first-tier offence has been committed. The subject message should relate to a Hong Kong resident or a person who was present in Hong Kong at the time of the disclosure though the disclosure itself does not need to take place in Hong Kong.
- (b) A cessation notice may be served on an individual who is present in Hong Kong; or a body of persons that is incorporated, established or registered in Hong Kong or has a place of business in Hong Kong (defined as "Hong Kong person" under the Bill). If the subject message is an electronic message, the notice can be served on a non-Hong Kong service provider who

has provided or is providing service (whether or not in Hong Kong) to any Hong Kong person.

- (c) The Commissioner may direct the person subject to a cessation notice to take a "cessation action" within a designated time period. Such actions may include steps to remove the subject message from the electronic platform on which the message is published, or stop or restrict access to the message or even the relevant electronic platform, or discontinue the hosting service for any part or the whole of the relevant electronic platform, so as to cease or restrict the subject disclosure.
- (d) The Commissioner, however, may exercise this power only if it has reasonable ground to believe that the person on whom a cessation notice is to be served is able to take the cessation actions as directed.
- (e) The person on whom a cessation notice is served or anyone affected by the notice may appeal to the Administrative Appeals Board (AAB) within 14 days after the notice is served. However, notwithstanding the appeal process, the notice will remain effective pending the AAB's decision and must still be complied with within the designated timeframe.
- (f) Indeed, non-compliance with a cessation notice is an offence, which carries a maximum penalty of a level-5 fine and imprisonment for two years on the first conviction.
- (g) It is, however, a defence for a person charged with the offence to establish that he had a reasonable excuse for contravening the cessation notice; or alternatively, it was not reasonable to expect him to comply with the cessation notice (i) having regard to the nature, difficulty or complexity of the cessation action concerned; (ii) because the technology necessary for complying with the cessation notice was not reasonably available to him; (iii) because there was a risk of incurring substantial loss to or otherwise substantially prejudicing the right of a third party; or (iv) because there was a risk of incurring a civil liability arising in contract, tort, equity or otherwise.

This will potentially allow the Commissioner to serve a cessation notice on online and technology firms globally which provide services to the public in Hong Kong,

<sup>4</sup> Section 64(4)(d) of the existing PDPO.

provided that the Commissioner reasonably believes that these firms are able to take the steps as required in the notice. Such firms may include operators of social networking sites, online search engine operators and internet service providers. It does not matter whether they have offices in the city. However, if they do (for example) have a branch office in Hong Kong, the branch office could be made the recipient of a cessation notice. If the branch office is only made up of administration and support personnel, a question may arise to whether the branch office has the ability to comply with a cessation notice.

By way of an example, local administrative staff of a social networking site operator may not have the authority or ability to take down the doxxing content from the platform which is hosted and managed overseas. It would be debatable whether the branch office, in the circumstances, is obliged to procure compliance of the notice by its headquarters when it is not able to directly remove the content.

Furthermore, a service provider, when served with a cessation notice, may be faced with difficult choices, leaving aside whether it has the ability to comply with it. It may be necessary for the service provider to challenge the cessation notice through an appeal if compliance with it will likely lead to lawsuits from third parties. However, as mentioned above, the service provider will still be obliged to comply with the notice within the specified timeframe (which is unlikely to be long) pending the results of the appeal. Consequences for non-compliance could be severe and depends very much on whether one of the defences available can be established.

It is worth mentioning that under Hong Kong law, if the person who commits the offence is a corporation, any director or officer of the corporation whose consent or connivance contributed to the commission of the offence, commits the same offence<sup>5</sup>. Hence, it is possible for personal liability to attach to the management of a company where he or she is responsible for causing a failure by the company to comply with a cessation notice.

Notwithstanding the above, it is comforting to hear from the Secretary for Constitutional and Mainland Affairs, Erick Tsang Kwok-wai that the anti-doxxing law only

<sup>5</sup> Section 101E of the Criminal Procedure Ordinance (Cap. 221).

<sup>6</sup> Section 61(1) of the existing PDPO and the proposed new sections 64(3A) and (3B) of the PDPO.

<sup>7</sup> The proposed new section 66 of the PDPO.

aims to target those who maliciously leak other's personal information rather than intermediate service providers, and that only persons with the ability to remove doxxing materials would be asked to do so.

### **New investigative, enforcement and prosecutorial powers**

To combat doxxing activities and enforce the disclosure offences under section 64 of the PDPO<sup>6</sup> more effectively, the Government proposes that the Commissioner be given more investigative and enforcement tools which are comparable to those available to other law enforcement agencies and regulators, such as the Police and the Securities and Futures Commission. In relation to a "specified investigation" (which effectively means an investigation into the disclosure offences and ancillary offences<sup>7</sup>), the Commissioner or a prescribed officer<sup>8</sup> are proposed to be conferred with the following powers:

- (a) Power to compel production of documents and information relevant to the investigation;
- (b) Power to apply to a magistrate for a warrant to enter and search premises, and seize materials in the premises which contain evidence for the investigation;
- (c) Power to apply to a magistrate for a warrant to access, detain, decrypt and search for any materials stored in an electronic device that the Commissioner reasonably suspects to be or contain evidence for the investigation;
- (d) Power to access an electronic device without warrant where it is not reasonably practicable to obtain a warrant, if it is reasonably suspected that the relevant offence has been committed or is about to be committed and the electronic device contains evidence for the investigation;
- (e) Power to stop, search and arrest, without warrant, anyone who is reasonably suspected to have committed the relevant offences, and to use reasonable force to effect the search or arrest if the subject person resists or attempts to evade the search or arrest; and
- (f) Power to apply for an injunction where a person has engaged, is engaging or is likely to engage in

<sup>8</sup> Prescribed officer means a person employed or engaged by the Commissioner pursuant to section 9(1) of the PDPO as the Commissioner thinks fit to assist him in the performance of his functions, and the exercise of his powers under the PDPO.

conduct that would constitute a disclosure offence.

The Government proposes that persons who, without lawful excuse, fail to comply with the Commissioner's document requests, provides false or misleading information to the Commissioner, or obstruct, hinder or resist the exercise of the above powers to search and arrest, shall be liable for an offence. The Commissioner shall have the power to prosecute such offences and the offence of conspiracy to commit such offences summarily.

It is also proposed that the Commissioner may prosecute the first-tier offence summarily. This means that more severe cases will be referred to the Police or the Department of Justice.

### Next steps

As at the time of this article, the Bill has passed its First Reading at the Legislative Council. A Bills Committee has been formed to study the Bill before the Second Reading. The Bill is expected to go through the Legislature before October 2021.

Whilst the Bill has yet to be passed by the Legislature, in view of the possibility that the Commissioner will be given wide investigative and enforcement powers, it is advisable for corporates to make a head start on formulating internal protocols and training programs so that local employees are well equipped to deal with cessation notices, requests for production of documents, searches, and seizures of materials (including electronic devices).

## CONTACT



**WYNNE MOK**  
PARTNER  
T: +852 2901 7201  
E: [wynne.mok@slaughterandmay.com](mailto:wynne.mok@slaughterandmay.com)



**JASON CHENG**  
ASSOCIATE  
T: +852 2901 7211  
E: [jason.cheng@slaughterandmay.com](mailto:jason.cheng@slaughterandmay.com)



**RUBY CHIK**  
ASSOCIATE  
T: +852 2901 7292  
E: [ruby.chik@slaughterandmay.com](mailto:ruby.chik@slaughterandmay.com)



**KATHLEEN POON**  
ASSOCIATE  
T: +852 2901 7358  
E: [kathleen.poon@slaughterandmay.com](mailto:kathleen.poon@slaughterandmay.com)

**London**  
T +44 (0)20 7600 1200  
F +44 (0)20 7090 5000

**Brussels**  
T +32 (0)2 737 94 00  
F +32 (0)2 737 94 01

**Hong Kong**  
T +852 2521 0551  
F +852 2845 2125

**Beijing**  
T +86 10 5965 0600  
F +86 10 5965 0650

Published to provide general information and not as legal advice. © Slaughter and May, 2021.  
For further information, please speak to your usual Slaughter and May contact.

[www.slaughterandmay.com](http://www.slaughterandmay.com)