BCLP. Client Intelligent

Insights

PART 6 OF 6: AMENDMENTS TO HONG KONG DATA PROTECTION LAW TO COVER DOXXING

Aug 03, 2021

SUMMARY

In light of the prevalence of doxxing and cyber harassment in Hong Kong, the Hong Kong government is keen to step up the efforts to curb the dissemination of personal data which is done to harass or harm to data subjects. It should be noted that a new doxxing offence and a series of PCPD empowerment provisions are under consideration.

This is last post of the series of six articles in which we discuss the proposed amendments to the data protection regime in Hong Kong. In this sixth part, we discuss the part of the proposed amendments to the Personal Data (Privacy) Ordinance ("PDPO") that are targeted at the increase in doxxing activities.

See links below for our previous articles on the proposed amendments:

- Part 1 of 6: our first article set out an overview of the six proposed amendments and included a discussion of the proposed introduction of a mandatory data breach notification mechanism.
- Part 2 of 6: our second article on the requirement for the formulation of a clear data retention policy.
- Part 3 of 6: our third article on the imposition of administrative penalties.
- Part 4 of 6: our fourth article on the regulation of data processors.
- Part 5 of 6: our fifth article on the widening of the definition of "personal data".

Introduction and Background

Doxxing and cyber harassment have been the subject of quite a lot of discussion and scrutiny in Hong Kong in recent years. Some commentators opine that doxxing acts "weaponise" personal

data and have caused great harm to people who fall victim to these intrusive acts.

The Hong Kong government and the Office of the Privacy Commissioner for Personal Data ("PCPD") take doxxing very seriously. One of the major considerations which spurred the efforts for a major overhaul of the Personal Data (Privacy) Ordinance ("PDPO") was the need to combat the acts of doxxing.

The acts of doxxing very often are done via internet platforms. In the past decade, there has been an emergence of online content hosts such as social media platforms and discussion forums. Data proliferation (i.e. a large amount of data content being stored by governmental organisations, businesses and online content hosts) has given doxxers an unprecedented amount of "raw materials" upon which to seek to prey.

According to statistics published on 17 May 2021[1], between June 2019 and April 2021, there were over 5,700 doxxing-related complaints received or uncovered by the PCPD. Over 1,460 cases which involved suspected criminal doxxing were referred to the Police for investigation. Only 17 suspects subsequently were arrested and only two ended up being convicted.

The obvious disparity in the numbers is thought by the Hong Kong government to have been due to inadequacies in Hong Kong's data protection law.

The Current Law and Why it is Not Good Enough

Section 64(2) of the PDPO provides that a person commits an offence, liable upon conviction to a fine of HK$1,000,000 and to imprisonment for five years if "(a) the person discloses any personal data of a data subject which was obtained from a data user without the data user's consent"; and (b) the disclosure causes psychological harm to the data subject" (emphasis ours).

Under the current legal regime, the PCPD recognises two forms of doxxing acts – criminal doxxing and non-criminal doxxing. Doxxing acts, even if in breach of data protection principles, but which do not cause psychological harm to data subjects, are non-criminal. The PCPD may issue enforcement notices to data users to require remedial actions. Doxxing acts which do cause psychological harm to victims are referred to as "criminal doxxing", and these cases are likely to be referred to the Police for further investigation and enforcement.

Section 64(2) of the PDPO currently is the only legal basis for the prosecution of doxxing. The Hong Kong government recognises that this provision is not targeted at doxxing and cyber harassment. It simply is the closest and the most relevant provision available under the current PDPO.

As emphasised above, section 64(2) of the PDPO hinges upon whether the data being disseminated was obtained with or without the relevant data user's consent. In the majority of doxxing cases which involve the use of online platforms, the offending data most likely was collected by internet platform providers and/or online content hosts under their respective privacy policies. The recent

surge of doxxing cases has involved multiple reposting on social media and messaging platforms, making it extremely difficult or even impossible for investigators to trace the relevant "data users" in respect of the offending content, not to mention ascertaining whether or not the data in question was obtained "without the data user's consent".

Aside from the difficulty in tracing the data users, the hands of the PCPD also are tied in the following ways:

- When faced with offending content published online, the PCPD only could write to the relevant online content hosts to request that the offending content be removed. It lacks the statutory power to order any mandatory removal.
- The PCPD does not have jurisdiction over overseas online content hosts.
- The PCPD does not have the power or standing to represent victims in court proceedings (for example, to apply for an injunction to restraint doxxing activities).
- The PCPD does not have the power to conduct criminal investigations. Suspected cases have to be referred to the Police for further action.
- The PCPD does not have the power to issue legally enforceable injunctive orders to require internet platform providers or online content hosts to disclose the identity of doxxers responsible for the offending content.

The Key to Change – From the "Data User's Consent" to the "Data Subject's Consent"

The Hong Kong government has proposed to introduce an all-new provision under the existing section 64 which criminalises the specific act of doxxing. The proposed provision provides that:-

> *"A person commits an offence if the person discloses any personal data of a data subject without the data subject's consent,*
>
> *(a) with an intent to threaten, intimidate or harass the data subject or any immediate family member, or being reckless as to whether the data subject or any immediate family member would be threatened, intimidated or harassed; or*
> *(b) with an intent to cause psychological harm to the data subject or any immediate family member, or being reckless as to whether psychological harm would be caused to the data subject or any immediate family member;*
>
> *and the disclosure causes psychological harm to the data subject or any immediate family member." (emphasis ours)*

The proposed provision is technology-neutral. It takes away the burden of tracing the identity of data users by shifting the focus to the data subject's consent. This formulation of the proposed

provision is targeted to capture personal data which, according to the Hong Kong government, was "recklessly dispensed and repeatedly reposted on online platforms". Under this new provision, if it is established that the victim never consented to the dissemination of his personal data, the doxxer can be liable regardless of where and how the doxxer obtained such data.

The Intention to Cause Harm

The proposed provision also comes with a relatively low threshold for the commission of criminal doxxing when compared to the positions adopted by New Zealand and Singapore[2]. New Zealand criminalises doxxing acts which are done with the intention to cause serious emotional distress, provided that such acts would cause harm to an ordinary person (i.e. objective test) and do indeed cause harm to the victim (i.e. subjective test)[3]. Singapore criminalises doxxing acts which were committed with the direct intent to cause harassment, alarm or distress to another person[4]. Under Hong Kong's proposed provision, a doxxer who does not possess a relevant direct intent still can be found guilty if the lower threshold of recklessness is satisfied.

The offence proposed by the Hong Kong government captures a comparatively wide range of doxxing activities and come with a higher maximum fine for infringement[5].

Whether or not the communication is in the interest of the public is one of the factors which the New Zealand courts are required (by law) to take into account when deciding what order is to be made against the doxxer[6]. New Zealand courts also are expressly required to act consistently with its Bill of Rights Act 1990[7]. Under the proposed new offence, similar safeguards to ensure the balance of rights come in the form of statutorily recognised defences. A person charged with this offence may rely on a list of defences, including that the disclosure was in the public interest and/or for the purpose of a news activity.

Empowering the PCPD

Hong Kong recognises the fact that fairly limited powers have been given to the PCPD to investigate and enforce breaches of the PDPO. The Legislature is keen to step up the efforts against doxxing by empowering the PCPD in multiple ways so that the PCPD's expertise in the area of data privacy protection can be better utilised.

The proposed additions to the PCPD's powers include the following:

(a) **Power to conduct criminal investigation**. This includes (i) the power to request information, documents and items from any person, (ii) the power to require any person to answer relevant questions, (iii) the power to apply to the court for entry into any premises, and (iv) the power to and seize documents and/or items, when the PCPD has reasonable grounds to believe that a contravention of section 64 of the PDPO has been or is being committed.

(b) **Power to initiate prosecution**. This is a proposed right for the PCPD to prosecute in its own name for suspected contraventions of section 64 offences or for failure to comply with the PCPD's investigative requests.

(c) **Power to demand rectification of doxxing acts**. This is a proposed power for the PCPD to issue Rectification Notices to any person who provides services in Hong Kong to Hong Kong residents irrespective of where that person is situate, for rectification actions to be done before a prescribed deadline. This amendment was proposed to address the facts that there are no geographical constraints in the Internet and that offending content can be published on overseas online content platforms. Defence and appeal mechanisms also have been proposed alongside this proposed power.

(d) **Power to apply for court injunctions**. This proposed power is intended to curb the occurrence of large-scaled or repeated doxxing incidents targeted at specific persons or groups.

Concluding comment

The relatively large amount of information publicly available in relation to Hong Kong's proposed amendments to prevent doxxing (relative to other proposed amendments to the PDPO) demonstrate the government's strong commitment to curb the recent prevalence of doxxing acts in Hong Kong.

The proposed new doxxing offence requires a relatively less stringent test with regard to the intention to cause harm when compared to other jurisdictions. Other proposed amendments discussed above are aimed at giving the PCPD wide-reaching (and potentially extra-territorial) enforcement powers intended to eradicate doxxing acts with improved efficiency and speed.

These amendments, if passed and enacted as currently proposed, will provide the statutory framework for increased "policing" by the PCPD. The strength and frequency of investigative and enforcement actions with regard to doxxing also are expected to increase.

---

1. See LC Paper No. CB(4)974/20-21(03) available here.
2. The government has considered the positions adopted by New Zealand and Singapore on the criminsation of doxxing. See paper no. IN09/19-20 "Measures to address doxxing in selected places" prepared by the Research Office of the Legislative Council Secretariat, available here.
3. Section 22(1) of New Zealand's Harmful Digital Communications Act 2015.
4. Section 3 of Singapore's Protection from Harassment Act.
5. About 3.87 times the maximum penalty under New Zealand's law and 34.8 times the maximum penalty under Singapore's law (for first time offenders who are natural persons).
6. Section 19(5)(g) of New Zealand's Harmful Digital Communications Act 2015.
7. Section 19(6) of New Zealand's Harmful Digital Communications Act 2015.

RELATED CAPABILITIES

- Data Privacy & Security
- Employment & Labor
- Corporate

MEET THE TEAM

Glenn Haley

Co-Author, Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450
