350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: 212-290-4700
Fax: 212-736-1300; 917-591-3452

January 17, 2020

HUMAN RIGHTS WATCH

HRW.org

Hon CHEUNG Kwok-kwan, JP
Chairman
Panel on Constitutional Affairs
panel_ca@legco.gov.hk

CC:
Mr. NIP Tak Kuen, Patrick, JP
Secretary for Constitutional & Mainland Affairs
scmaoffice@cmab.gov.hk

Re: Review of the Personal Data (Privacy) Ordinance

Dear Mr. Cheung,

Human Rights Watch is an international nongovernmental organization that investigates and reports on a wide range of human rights issues, including privacy, in over 90 countries. We request that you distribute this letter to members of the Legislative Council (LegCo) Panel on Constitutional Affairs who will be reviewing the Personal Data (Privacy) Ordinance (PDPO) on January 20.[1]

We welcome the review of the PDPO, which was adopted in December 1996, but has not been updated since 2012. The PDPO was largely modelled after the European Data Protection Directive, which was adopted in 1995 but replaced in 2018 by the European General Data Protection Regulation (GDPR). The GDPR gives people enhanced rights protections in the collection and use of personal data by governments and the private sector as people's lives leave increasing digital trails.

We broadly welcome the proposed direction of the PDPO review as outlined in LC Paper No. CB(2)512/19-20(03), which introduces a mandatory data breach notification mechanism, requiring data users to formulate clear retention policies, stronger penalties, and direct regulation of data processors. Yet we are concerned that the proposal fails to offer more comprehensive privacy protections, as the GDPR has done. We would like to draw your attention to the following areas:

1) Broaden the definition of personal data and protect sensitive data

We agree with the proposed expansion of the definition of personal data, shifting from only data that relates to an "identified" person to that of an

[1] Panel on Constitutional Affairs Meeting on Monday, 20 January 2020, at 2:30 pm in Conference Room 1 of the Legislative Council Complex Revised Agenda, January 13, 2020, https://www.legco.gov.hk/yr19-20/english/panels/ca/agenda/ca20200120.htm (accessed January 17, 2020).

"identifiable" natural person. That means even data that does not directly identify named persons—such as a license plate number of a private vehicle—but could still help identify them, will be covered by the revised PDPO. This new definition will encompass online and device identifiers (like IP addresses, cookies, or device IDs), location data, user names, and pseudonymous data.

But the proposed amendments to PDPO should also make a distinction between general personal data and data that is particularly sensitive, as the GDPR does. The latter allows the processing of sensitive personal data—including information revealing someone's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, health, and biometrics—only under specific, strict conditions.[2]

We are particularly concerned about the collection of biometrics, which are unique identifiers that cannot be changed during one's lifetime. Facial images and DNA are particularly problematic, as the former allows governments and companies to surreptitiously identify and track large swaths of the public without their consent, and the latter reveals sensitive information about people, including to whom they are related. The Office of the Privacy Commissioner for Personal Data ("PCPD") shared this concern, stating in July 2015 that the "[c]ollection and use of biometric data for consumer applications have been on the increase" and issued a Guidance Note specifically on the collection of such "sensitive" data.[3] It is time for the government to elevate such concerns from a non-enforceable Guidance Note into a legislative amendment.

Human Rights Watch calls on the Hong Kong government to impose a moratorium on government's use of facial recognition until comprehensive regulatory frameworks are in place. The European Commission, for example, is deliberating over special rules that would tightly govern facial recognition.[4]

2) Strengthen the rights of people whose data is collected

Human Rights Watch is concerned that the proposed amendments to the PDPO do not significantly strengthen the rights of people whose information is collected beyond what already exists in the current PDPO.

- *Consent:* An important component of the GDPR is its requirement that people must give their explicit consent before their personal data can be collected, used, or shared. The request for consent must be clearly distinguishable, in an intelligible and easily accessible form, and use clear and plain language.[5] In other words, the request for consent has to be easy to find, and easy to understand.

---

[2] GDPR, art. 9.

[3] PCPD, New Guidance for the Responsible Collection and Use of Biometric Data , July 20, 2015, https://www.pcpd.org.hk/english/news_events/media_statements/press_20150720.html.

[4] Mehreen Khan, "EU plans sweeping regulation of facial recognition," *Financial Times*, August 22, 2019, https://www.ft.com/content/90ce2dce-c413-11e9-a8e9-296ca66511c9.

[5] GDPR, art. 6(1)(a).

    - The PDPO requires that people be informed. But it does not require explicit consent for data collection except when the data collected is used for new purposes or when it is transferred for direct marketing.

- *Right to erasure:* Under the GDPR, people can ask a company to disclose what personal data it holds about them and receive it free of charge and then in some circumstances require the company to delete it.
    - The PDPO allows people to access information held about them, and the proposed amendments require companies to have a clear data retention policy, which is welcomed. However, the PDPO does not give people the right to have their information removed or to be de-indexed from search engines.

- *Restrictions on cross-border data transfer:* Under GDPR, EU personal data cannot be transferred to countries outside the EU unless the data processor shows that the data will be protected in ways "essentially equivalent" to protections in Europe.
    - While there are restrictions to cross-border data transfer under section 33 of the PDPO, they have not come into effect. The PCPD issued a guidance note on the matter on December 29, 2014, stating that the "the issue of regulating cross-border data flows is becoming more acute than ever before," but the Hong Kong "Administration has not set a firm date for implementation of section 33."[6] Given Hong Kong's role as an international financial center, having a rigorous, enforceable cross-border regime is vital.

- *Right to object to processing:* The GDPR gives people the right to object to the processing of their personal data in certain circumstances.
    - The PDPO does not give people such rights, and only allows people to opt out from direct marketing activities.

Human Rights Watch recommends that the Hong Kong government give people these rights, requiring explicit consent before their data can be used and the right to withdraw such consent at any time, empowering people to erase their data and to object to processing, and restricting cross-border data transfers unless the data will be given equivalent privacy protections.

However, even if the PDPO is amended to significantly improve protections of personal data, it will unlikely curtail large-scale government surveillance if the PDPO continues to allow broad exemptions when the data is being used for the detection or prevention of crime. Hong Kong's outdated surveillance legislation, the Interception of Communications and Surveillance Ordinance (ICSO), further compounds the problem. The ICSO:

- Regulates only telecommunications and postal interception, but not newer forms of communications including social media or instant messaging.[7]

---

[6] PCPD, PCPD Publishes Guidance on Personal Data Protection in Cross-border Data Transfer, December 29, 2014, https://www.pcpd.org.hk/english/news_events/media_statements/press_20141229.html.

[7] Kris Cheng, Hong Kong gov't lagging behind in surveillance laws and routine disclosure, HKU researchers say, *Hong Kong Free Press*, https://www.hongkongfp.com/2018/02/14/hong-kong-govt-lagging-behind-surveillance-laws-routine-disclosure-hku-researchers-say/ (accessed January 17, 2020).

- Contrary to practices in other similar jurisdictions that respect the rule of law, the ICSO does not require the police to produce a court order or other form of judicial authorization when demanding an individual's personal data from a company, or even require detailed guidance or a code of practice for responding to user data requests.

Hong Kong government departments also give police personal information they hold on demand. While internal procedures exist for responding to such requests, there is no code of practice or detailed guidance publicly available to ensure such disclosure decisions balance law enforcement interests and privacy rights. Human Rights Watch calls on the LegCo to also update the ICSO to address these loopholes.

In China, the Chinese government has implemented mass surveillance systems across the country.[8] Using a combination of national identification cards, "real name registration" requirement, networks of sensory systems including closed-circuit surveillance cameras (CCTV), artificial intelligence technologies including facial recognition, mass collection of DNA, and big data systems such as the Integrated Joint Operations Platform (IJOP) in Xinjiang, the police aim to monitor the population around the clock, and use technologies to pick out people whom they consider as "problematic."[9]

In recent months, the public in Hong Kong has shown strong concerns about such systems expanding into Hong Kong, especially as the government embraces a range of Smart City initiatives.[10] It is imperative that the Hong Kong authorities assuage these fears by strengthening privacy rights and the regulatory framework governing the collection of personal data by both the government and the private sector.

We welcome an opportunity to discuss these issues with you at your convenience, and wish you a successful legislative review.

Yours sincerely,

Sophie Richardson
China Director
Human Rights Watch

---

[8] For a collection of articles on this topic, see Human Rights Watch, Mass Surveillance in China, https://www.hrw.org/tag/mass-surveillance-china.

[9] Maya Wang, "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," Human Rights Watch, May 1, 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance.

[10] Ephrat Livni, Hong Kong protestors are attacking smart lampposts, Quartz, August 25, 2019, https://qz.com/1694684/hong-kong-protestors-are-attacking-smart-lampposts/ (accessed January 17, 2020).