立法會
Legislative Council

LC Paper No. CB(4)974/20-21(04)

Ref : CB4/PL/CA

Panel on Constitutional Affairs

Background brief prepared by the Legislative Council Secretariat for the meeting on 17 May 2021

Proposed amendments to the Personal Data (Privacy) Ordinance (Cap. 486)

Purpose

This paper provides background information on the proposed amendments to the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO"). It also summarizes the discussion of the Panel on Constitutional Affairs ("the Panel") on the latest review of PDPO.

Background

Personal Data (Privacy) Ordinance

2. PDPO, having come into force since 1996, aims to protect the individual's right to privacy with respect to personal data. PDPO applies to any data relating directly or indirectly to an individual, from which it is practicable to ascertain the identity of the individual and which is in a form in which access to or processing is practicable. Users of personal data in both public and private sectors are subject to the provisions of PDPO.

3. The Administration conducted a comprehensive review of PDPO with the support of the Privacy Commissioner for Personal Data ("PCPD"), and consulted the public from August to November 2009 on proposals arising from the review. The Administration published the consultation report in October 2010 [LC Paper No. CB(2) 37/10-11(02)] and further consulted the public on the legislative proposals from October to December 2010. The Report on Further Public Discussions on Review of PDPO was published in April 2011. The Ordinance

was amended in mid-2012 and all the amended provisions have already come into operation.[1]

Latest review of the Personal Data (Privacy) Ordinance

4. When the Panel received a policy briefing by the Secretary for Constitutional and Mainland Affairs on 16 December 2019 on the policy initiatives of the Constitutional and Mainland Affairs Bureau ("CMAB") as announced in the 2019 Policy Address, the Administration advised that in view of the series of major personal data breach incidents which took place earlier, CMAB was actively reviewing and studying possible amendments to the PDPO jointly with PCPD to strengthen protection towards personal data privacy.[2] CMAB was focusing its study on several amendment directions, including:

(a) establishing a mandatory data breach notification mechanism;

(b) strengthening the regulation on data retention period;

(c) reviewing penalties of non-compliance with PDPO by raising relevant criminal fines and exploring the feasibility of introducing direct administrative fines;

(d) regulating data processors directly to strengthen protection towards personal data being processed; and

(e) amending the definition of "personal data" to cover information relating to an "identifiable" natural person.

---

[1] The Personal Data (Privacy) (Amendment) Ordinance 2012 ("Amendment Ordinance") was passed by LegCo on 27 June 2012. The Amendment Ordinance introduced amendments to PDPO, inter alia, to provide for regulation over the use of personal data in direct marketing and provision of personal data for use in direct marketing; to create a new offence for disclosure of personal data obtained without consent from data users; to empower PCPD to provide legal assistance to aggrieved data subjects in bringing proceedings to seek compensation from data users under PDPO; to impose a heavier penalty for repeated contravention of enforcement notices; and to create a new offence for repeated contravention of the requirements under PDPO for which enforcement notices have been served.

[2] Major personal data breach incidents in recent years included the incident of leakage of personal data of 9.4 million passengers as announced by Cathay Pacific Airways Limited on 24 October 2018 and suspected security loopholes in the TransUnion Limited's online procedures for obtaining personal credit information as reported by the press in November 2018.

Consultation with the Panel on Constitutional Affairs on the amendment directions

5. The Panel was consulted on the proposed legislative amendment directions at its meeting on 20 January 2020. Members were informed that the Administration was also studying how PDPO could be amended in order to curb doxxing behaviours more effectively. Directions under consideration included introducing legislative amendments to more specifically address doxxing, conferring on PCPD statutory powers to request the removal of doxxing contents from social media platforms or websites, as well as the powers to carry out criminal investigation and prosecution, etc. When the Panel received a briefing by PCPD on the work of the Office of PCPD on 18 January 2021, members also raised issues relating to the review of PDPO. The major views and concerns expressed by members are summarized below.

Scope of the latest review of the Personal Data (Privacy) Ordinance

6. Some members expressed concern that the proposed amendment directions outlined in the Administration's paper (LC Paper No. CB(2)512/19-20(03)) failed to address important issues discussed in the last review of PDPO in 2009, including granting criminal investigation and prosecution powers to PCPD, and enhancing protection of sensitive personal data. These members considered it necessary to bring Hong Kong's data protection regime on a par with international standards and urged that more comprehensive data privacy protections be introduced in PDPO by making reference to the General Data Protection Regulation ("GDPR") of the European Union. These members also urged the Administration to address data privacy challenges brought about by the development and application of various disruptive technologies (e.g. facial recognition and other biometric technologies, big data analytics, artificial intelligence and profiling). They expressed doubt that the proposed amendment directions appeared to mainly tackle the issue of doxxing.

7. The Administration explained that the spate of major personal data breach incidents in recent years had aroused public concerns about the adequacy of PDPO in protecting personal data privacy. In the light of this, the Administration had been reviewing and studying possible amendments to PDPO jointly with the Office of PCPD with a view to strengthening protection of personal data privacy. In view of the large number of doxxing incidents recently, the Administration considered it also necessary to examine how PDPO should be amended in order to curb doxxing behaviours more effectively. PCPD advised that in order to propose reasonably practicable proposals to amend PDPO, the Office of PCPD would make reference to relevant laws in other jurisdictions (including GDPR) and take into account local circumstances and needs.

Proposed mandatory data breach notification mechanism

8. Some members enquired about the notification threshold and mode of notification under the proposed mandatory data breach notification mechanism, which would require data user to notify PCPD and the relevant data subject of any data breach incident. They also enquired whether guidelines would be provided to data users in respect of the notification threshold and notification timeframe to facilitate compliance with the relevant requirements.

9. The Administration explained that details of the notification mechanism were proposed with reference to the relevant legislation and experience of other jurisdictions. To help reduce the damage caused to the affected data subjects, the data user would be required to notify PCPD within a specified timeframe (e.g. as soon as practicable and, under all circumstances, in not more than five business days) upon having become aware of a data breach, failing which the data user would be subject to penalties. The Administration was considering whether it was necessary to allow a specified period for the data user to investigate and verify the suspected data breach incident before making notification to PCPD within the specified timeframe. As regards the mode of notification, the Administration considered that while notification could be made more promptly and conveniently by phone or via other instant messaging applications, it would be more appropriate to require data users to make formal written notification providing relevant details of the data breach by email, fax or post.

Curbing doxxing behaviours

10. At the Panel meeting on 18 January 2021, some members expressed concern that while a large number of doxxing incidents had taken place since 2019, only a small number of convictions were brought under section 64 of PDPO, i.e. disclosure of personal data obtained without consent from the data user, causing psychological harm to the data subject. The Administration was urged to make appropriate amendments to the relevant section(s) of PDPO so as to tackle the problem of doxxing more effectively.

11. PCPD advised that the Government and the Office of PCPD were conducting an in-depth study on how PDPO should be amended in order to handle and regulate doxxing-related behaviour more effectively. Issues such as the definition of doxxing offence, criminal penalties, power to issue notice to remove doxxing content, evidential threshold and PCPD's statutory criminal investigation and prosecution powers were being examined. PCPD further advised that she was currently not vested with the power under PDPO to request the removal of doxxing contents from online platforms and websites. As such,

PCPD had to resort to writing to the platforms/websites concerned to seek their cooperation to do so.

12. With regard to the proposal of empowering PCPD to impose administrative fines under PDPO, some members enquired whether such fines could be imposed on organizations (e.g. social media platforms and website operators) which failed to prevent or stop/assisted in the publication and dissemination of leaked personal data, with a view to combating doxxing and cyberbullying more effectively.

13. PCPD advised that the proposal of imposing administrative fines would facilitate PCPD's tackling of non-criminal doxxing cases, which mainly involved contravention of the Data Protection Principles under PDPO. As for criminal doxxing cases involving intimidation or incitement which might cause psychological harm to the victims concerned, PCPD advised that difficulties had been encountered in tracking the doxxers and following up with the online platforms involved. To address this, the Government and the Office of PCPD were studying how PDPO should be amended in order to bring not only doxxers but also the platforms concerned under regulation.

14. Some members expressed concerns about possible abuse of the personal data contained in public registers maintained by the Government for doxxing-related purposes. These members suggested that PCPD should, in tandem with the review of PDPO, examine whether the current arrangements for access to public registers provided under the relevant legislation were compliant with the requirements of PDPO and recommend legislative amendments where appropriate. PCPD advised that the Office of PCPD would consider examining relevant issues with a view to making recommendations to the Government on ways to improve the protection of personal data contained in public registers.

Relevant Legislative Council questions in the current legislative session

15. At the Council meetings of 4 and 18 November 2020, Hon Alice MAK raised two written questions on "Measures against doxxing and cyber-bullying" and "Services for searching various registers and government records" respectively. The Administration's replies to these questions are in **Appendices I** and **II** respectively.

Recent development

16. The Administration will consult the Panel on the proposed amendments to PDPO at the next meeting on 17 May 2021.

Relevant papers

17. A list of the relevant papers on the Legislative Council website is in **Appendix III**.

Council Business Division 4
Legislative Council Secretariat
11 May 2021

Appendix I

Press Releases

LCQ7: Measures against doxxing and cyber-bullying
****

Following is a question by the Hon Alice Mak and a written reply by the Acting Secretary for Constitutional and Mainland Affairs, Mr Andy Chan, in the Legislative Council today (November 4):

Question:

From the eruption in the middle of last year of the disturbances arising from the opposition to the proposed legislative amendments to September 30 this year, the Office of the Privacy Commissioner for Personal Data (PCPD) handled a total of over 4 700 cases relating to doxxing. Among such cases, around 35 per cent of the persons who had been doxxed were police officers or their family members. In this connection, will the Government inform this Council:

(1) whether it knows (i) the number of requests for assistance received by PCPD since January of last year from persons claiming that they had been doxxed, with a breakdown by the background of the assistance seekers, (ii) the respective numbers of cases in respect of which PCPD had taken various follow-up actions (including (a) requesting the operators to remove illegal web links and (b) referring the cases to the Police for conducting criminal investigation), and (iii) the respective numbers of persons prosecuted and convicted;

(2) whether it has assessed if the current evidential threshold is too high for offences relating to doxxing;

(3) as the Government indicated in its reply to my question on January 8 this year that it was studying with PCPD the amendments to the Personal Data (Privacy) Ordinance (Cap. 486), so as to more specifically address the acts relating to doxxing, of the specific contents of the legislative amendments and the legislative timetable; and

(4) given that the Singapore authorities passed

the amendments to the Protection from Harassment Act last year, including introducing new offences and penalties, expanding the scope of redress for victims of cyber-bullying, and establishing the Protection from Harassment Court to expedite the handling of applications for redress, so as to address the problem of doxxing, and that the General Data Protection Regulation which took effect in the European Union in 2018 provides that an individual enjoys the right to erasure (also known as "the right to be forgotten") and is entitled to require organisations and enterprises to delete his or her personal data under specified circumstances, whether the Government will make reference to such practices and amend the local legislation to step up efforts in combating the acts of doxxing and cyber-bullying; if so, of the details (including the public consultation and legislative timetables); if not, the reasons for that?

Reply:

President,

After consulting the Security Bureau and the Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD), a consolidated reply to the question is set out as follows:

(1) The PCPD received the first complaint relating to doxxing on June 14, 2019. As at the end of September 2020, the PCPD has handled 4 714 doxxing-related cases, including complaints received as well as cases uncovered by the PCPD's proactive surveillance. Of these, 4 370 of the cases were handled before the end of 2019 and 344 were handled between January to September 2020. Victims of these doxxing cases come from different backgrounds. Among the cases, 1 657 involved police officers and their family members (representing around 35 per cent of the total number of cases), and 189 related to doxxing against government officials and public servants (representing around 4 per cent of the total number of cases). Besides public officers, members of the public who had allegedly expressed support to the Government or the Police (representing around 30 per cent of the total number of cases) while some members of the public after allegedly voiced opposition against the Government or the Police (representing around 31

per cent of the total number of cases) were also doxxed.

For cases where criminal elements might be involved, the PCPD will refer the doxxing cases to the Police for follow-up to facilitate criminal investigation and consideration of prosecution. According to section 64(2) of the Personal Data (Privacy) Ordinance (PDPO), a person commits a criminal offence if he/she discloses any personal data obtained from a data user without the data user's consent and such disclosure causes psychological harm to the data subject. The person who commits such offence is liable on conviction to a maximum fine of $1,000,000 and imprisonment for up to five years. As at the end of September 2020, the PCPD has referred 1 413 cases on suspicion of contravening section 64 of the PDPO, i.e. disclosing personal data obtained without consent from data users, to the Police for follow-up. The Police has to date arrested 17 individuals for alleged contravention of section 64 of the PDPO. On October 9, 2020, a defendant was convicted in the District Court of, among other charges, contravention of section 64(2) of the PDPO. This was the first conviction under section 64 of the PDPO.

Furthermore, on October 25, 2019, the High Court granted an injunction order restraining any person from using, publishing, communicating or disclosing personal data of any police officer(s) or their family members intended or likely to intimidate, molest, harass, threaten or pester any police officer(s) or their family members without consent of the persons concerned; from intimidating, molesting, harassing, threatening or pestering any police officer(s) or their family members; or from assisting, inciting, abetting or authorising others to commit any of these acts. As at the end of September 2020, the PCPD has referred 45 doxxing cases on suspicion of breaching the relevant injunction orders to the Department of Justice for further action. On June 17, 2020, a defendant was convicted in the High Court of civil contempt of court for disclosing personal data of a police officer and his family members on a social media platform. The defendant was sentenced to 28 days' imprisonment, suspended for one year. This was the first conviction for breaching the relevant injunction order following the court's granting

of the injunction orders to restrain any person from doxxing against police officers. On October 19, 2020, another defendant was convicted in the High Court of civil contempt of court for forwarding personal data of a police officer on a social media platform. The defendant was also sentenced to 28 days' imprisonment, suspended for one year.

Apart from referring the relevant cases to the Police for follow-up, the PCPD will also monitor and continue patrolling of online platforms, and enhance publicity and education efforts. The PCPD has also reminded operators of relevant websites, online social media platforms or discussion forums that they should prevent their platforms from being abused as a tool for infringing personal data privacy. It has also requested the operators concerned to issue on their platforms warnings to netizens that doxxing behaviour may violate the PDPO and may also constitute criminal offence. In respect of requesting operators to remove doxxing-related web links, as at the end of September 2020, the PCPD has sent 229 written requests to different operators of websites, online social media platforms and discussion forums requesting for the removal of 3 461 web links relating to doxxing. So far, 2 308 web links (67 per cent) have been removed. The PCPD will also enlist cooperation from regulatory authorities in other jurisdictions to combat doxxing on social media platforms.

(2) to (4) Drawing on the actual experience of investigation and prosecution in handling doxxing cases in the past, the Constitutional and Mainland Affairs Bureau and the PCPD have been studying concrete proposals in amending the PDPO to more effectively handle and regulate doxxing related behaviour. Our aim is to endeavour to complete formulation of concrete legislative amendment proposals within next year and to consult the Legislative Council Panel on Constitutional Affairs followed by commencing legislative drafting work on the amendment proposal. In the process, the PCPD will make reference to relevant laws in other jurisdictions (including Singapore, the European Union, Australia and New Zealand) in order to propose reasonably practicable legislative amendment proposals on areas such as the definition of

doxxing offence, penalties, evidential threshold, Privacy Commissioner for Personal Data's statutory criminal investigation and prosecution powers, while striking an appropriate balance among the protection of personal data privacy, freedom of expression and free flow of information when strengthening the combat against doxxing. Regarding the right to erasure (also named as "right to be forgotten") in the General Data Protection Regulation of the European Union, since the relevant topic is controversial, the PCPD will continue to closely monitor development and implementation of such in other jurisdictions in this regard before further considering the matter. At present, the existing PDPO already provides for the erasure of personal data under Data Protection Principle 2(2) in Schedule 1, and section 26 of the PDPO, specifying that a data user has the responsibility to take all practicable steps to erase personal data where the data is no longer required for the purpose for which it was collected.

Ends/Wednesday, November 4, 2020
Issued at HKT 16:35

NNNN

Appendix II

Press Releases

LCQ19: Services for searching various registers and government records

****

Following is a question by the Hon Alice Mak and a written reply by the Secretary for Constitutional and Mainland Affairs, Mr Erick Tsang Kwok-wai, in the Legislative Council today (November 18):

Question:

Regarding the services provided by the Government for searching various registers and government records which contain personal data (search services), will the Government inform this Council:

(1) of the number of applications for each type of search services in each of the past two financial years and, among them, the number of those rejected;

(2) whether the relevant government departments have imposed regulation and conducted random checks on the search services to prevent them from being abused; if so, of the details, and the respective numbers of persons prosecuted and convicted in the past five years for unlawful use of the personal data obtained through the search services;

(3) of the current requirements of the various search services in respect of the following: (i) whether the applicants are required to give reasons for the applications, (ii) whether there are restrictions on the types of applicants, and (iii) whether the types of data obtainable are dependent on the reasons for application and the types of applicants; whether the Government will comprehensively review such requirements with a view to preventing abuses of the search services;

(4) whether it will enact legislation or formulate a mechanism to enable a data subject to apply on reasonable grounds (such as personal safety being threatened) for classification of the data relating to him or her in a register or government record as confidential or non-public,

so that it does not fall within the scope of data which is obtainable from the search services; and

(5) of the measures in place to prevent personal data obtained through the search services from being used for improper purposes, such as doxxing?

Reply:

President,

Our consolidated reply to the Hon Alice Mak's question is as follows:

At present, Government public registers are maintained and managed by respective Government departments. The content available for public inspection is decided by respective departments having regard to the relevant legislation and policies with a view to achieving the purpose of the public register and at the same time suitably safeguarding personal data privacy. The Constitutional and Mainland Affairs Bureau does not have the search figures of the respective public registers.

Reviews are conducted from time to time by Government departments on the arrangements and other matters relating to the handling of public registers in the light of social development and public needs, with the aim to satisfy public needs and at the same time endeavour to safeguard the personal data privacy of data subjects and appropriately balancing freedom of speech and information flow. At present, according to section 64(2) of the Personal Data (Privacy) Ordinance (PDPO), a person commits an offence if he/she discloses any personal data obtained from a data user without the data user's consent and such disclosure causes psychological harm to the data subject. The person who commits such offence is liable on conviction to a fine of $1,000,000 and to imprisonment for five years. Since the social unrest in June last year, the Police has to date arrested 17 individuals for alleged contravention of section 64 of the PDPO. On October 9, 2020, one of the defendants was convicted in the District Court of, among other charges, contravention of section 64(2) of the PDPO. On November 3, 2020, the defendant was sentenced to 18 months' imprisonment, and

together with other convictions, received a sentence of imprisonment for a total of two years.

Ends/Wednesday, November 18, 2020
Issued at HKT 15:30

NNNN

Appendix III

Relevant documents on
Proposed amendments to the Personal Data (Privacy) Ordinance (Cap. 486)

Committee	Date of meeting	Paper
Panel on Constitutional Affairs	16.12.2019 (Item IV)	Agenda Minutes
	20.1.2020 (Item III)	Agenda Minutes
Legislative Council	4.11.2020	Official Record of Proceedings Pages 97 to 101
	18.11.2020	Official Record of Proceedings Pages 114 to 116
Panel on Constitutional Affairs	18.1.2021 (Item IV)	Agenda Minutes

Council Business Division 4
Legislative Council Secretariat
11 May 2021