立法會
Legislative Council

LC Paper No. CB(4)361/2022(04)

Ref : CB4/PL/CA

Panel on Constitutional Affairs

Updated background brief prepared by the Legislative Council Secretariat for the meeting on 16 May 2022

Work of the Office of the Privacy Commissioner for Personal Data

Purpose

This paper summarizes previous discussions held by the Panel on Constitutional Affairs ("the Panel")[1] regarding the work of the Office of the Privacy Commissioner for Personal Data ("PCPD").

Background

2. The Office of PCPD is a statutory body responsible for overseeing the enforcement of the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO") which protects the privacy of individuals in relation to personal data. The Office of PCPD is headed by PCPD appointed by the Chief Executive. According to section 5(4) of PDPO, PCPD shall hold office for a period of five years and shall be eligible for reappointment for not more than one further period of five years. Section 8 of PDPO prescribes the functions and powers of PCPD as set out in **Appendix 1**. The Office of PCPD is funded mainly by recurrent subvention from the Government. Ms Ada CHUNG Lai-ling was appointed in July 2020 as the new PCPD with effect from 4 September 2020 for a term of five years, succeeding Mr Stephen WONG Kai-yi, the former PCPD.

The Personal Data (Privacy) (Amendment) Ordinance 2021

3. In September 2021, the Personal Data (Privacy) (Amendment) Bill 2021 was passed by the Legislative Council ("LegCo"). The Personal Data (Privacy) (Amendment) Ordinance 2021 ("Amendment Ordinance") came into effect on

[1] With effect from the 2008-2009 legislative session, the policy area of personal data protection has been transferred from the Panel on Home Affairs to be placed under the purview of this Panel.

8 October 2021. The Amendment Ordinance aims to combat unlawful doxxing acts in three aspects: (1) criminalize doxxing acts as new offences targeting malicious acts of disclosing personal data of the data subject without his/her consent, with an intent or being reckless as to whether specified harm would be caused to the data subject or his/her family member; (2) empower PCPD to carry out criminal investigations and institute prosecution towards doxxing-related offences; and (3) confer on PCPD statutory powers to serve notices to those who are able to take a cessation action, directing them to cease disclosure of doxxing contents (cessation notices).

Major issues discussed at Panel meetings

4. It is the usual practice of the Panel to receive a briefing by PCPD on the work of the Office of PCPD in each legislative session. The major issues raised at the relevant meetings are summarized below.

Privacy issues arising from the Coronavirus Disease 2019 ("COVID-19") epidemic

5. Members requested PCPD to clarify whether the Data Protection Principles and relevant requirements under PDPO would be violated if the Administration added a function of tracing the location of users to the "LeaveHomeSafe" mobile application ("app") for anti-epidemic purposes. PCPD explained that PDPO was principle-based and did not prohibit the collection, holding, processing or use of personal data for anti-epidemic or public health purposes, including the addition of the contact tracing function to the "LeaveHomeSafe" app. PCPD pointed out that when collecting personal data, relevant departments had to ensure compliance with the requirements of PDPO, including the requirements that only necessary, adequate but not excessive personal data should be collected. PCPD also pointed out that data subjects should be informed of the data collected, the purposes for which the data would be used, and to whom the data might be transferred (such as the Department of Health). In addition, section 59 of PDPO provided that if public health issues were involved, information such as the identity, health status and location of data subjects could be exempted from the relevant data use principles. The Administration advised that to effectively control the current severe epidemic situation in Hong Kong, the Administration would strive to strike an appropriate balance between controlling the epidemic and protecting personal data privacy when formulating anti-epidemic measures.

6. Since the outbreak of the COVID-19 epidemic, the use of online videoconferencing software has become popular. Members expressed concern that certain software was said to have a number of data security loopholes

(e.g. lack of end-to-end encryption) and was thus vulnerable to hacking attacks. Members enquired about the measures taken by the Office of PCPD to prevent abuse and misuse of personal data by software developers and operators.

7. The former PCPD advised that the Office of PCPD had issued guidelines on compliance with PDPO in developing software and apps. To promote the adoption of "Privacy by Design" and "Privacy by Default" as core considerations of enterprises when developing information and communications technology ("ICT") systems, the Office of PCPD and Singapore's Personal Data Protection Commission had released a jointly-developed guide to assist enterprises in applying "data protection by design" principles by offering practical guidance for all phases of software development and good practices for data protection for ICT systems. Moreover, the Office of PCPD had provided guidance to users of videoconferencing software in general through different channels. It had also written to schools to alert them of the risks when using videoconferencing software as an online teaching and learning platform.

Review of the Personal Data (Privacy) Ordinance

8. The Panel expressed the view that the regulation of data protection should be enhanced through amendments to PDPO in the wake of a few major incidents of personal data leakage in late 2018. Members were particularly concerned that there was no mandatory requirement under PDPO for an organization to file data breach notifications whether to the Office of PCPD or to its affected clients.

9. The former PCPD advised that the Office of PCPD had drawn up initial recommendations on the review of PDPO regarding the enhancement of data breach notification arrangements, retention and disposal of personal data by data users, penalties for non-compliance with PDPO, and regulation of data processing activities by data processors (such as cloud service providers), etc. The Administration subsequently embarked on a review and studied possible amendments to be made to PDPO jointly with the Office of PCPD, with a view to strengthening the protection for personal data. In June 2019, PCPD put forward to the Government its preliminary recommendations on PDPO amendments. The Administration then consulted the Panel on the preliminary amendment directions. The proposed directions encompassed issues relating to the definition of personal data, conferring on PCPD criminal investigation and prosecution powers (including enhanced powers to deal with offences like doxxing), instituting a mandatory data breach notification system, empowering PCPD to administer administrative fines and increasing the maximum level of criminal fines, as well as requiring organizational data users to formulate a

clear retention policy which should include stipulating the maximum retention period for personal data, etc.

10. Members noted that since June 2019, there had been an upsurge of doxxing activities. In order to curb doxxing behaviours more effectively, the Administration in July 2021 submitted to LegCo the Personal Data (Privacy) (Amendment) Bill 2021 which introduced new offences under Cap. 486 as well as new enforcement powers of PCPD as detailed in paragraph 3 above.

11. At the Panel's policy briefing-cum-meeting on 10 February 2022, members enquired about the enforcement by the Office of PCPD of the Amendment Ordinance after it had come into operation in October 2021. PCPD advised that relevant enforcement actions had started to bear fruit. The Office of PCPD made the first arrest for a suspected doxxing offence on 13 December 2021 and was seeking advice from the Department of Justice on the case. Prosecution would be instituted when there was sufficient evidence. In addition, the Office of PCPD was conducting criminal investigations into 40 cases, and had issued more than 350 cessation notices to 12 online platforms, involving over 1 700 doxxing messages.

Public education on privacy protection

12. Some members considered that many of the promotion and education activities conducted by the Office of PCPD could hardly arouse the interest of the general public in personal data protection. They suggested that efforts should be targeted at promoting public awareness of the legal responsibility of doxxing acts and the importance of personal data protection in new and innovative ways.

13. The former PCPD advised that the Office of PCPD had launched new accounts and revamped its page/channel on various social media platforms (e.g. Instagram, Twitter, Facebook and YouTube) in early April 2020, with a view to enhancing the dissemination of updated information on protection of personal data privacy to the general public, particularly the younger generation and those who preferred mobile devices to conventional media channels. Through these platforms, the latest privacy issues of public concern would be explained to the public in a plain language and with the help of visual illustrations and videos.

14. At the Panel's policy briefing-cum-meeting on 10 February 2022, PCPD stated that the Office of PCPD was conducting publicity and educational activities on the regulation of doxxing behaviour under the amended PDPO. The number of complaints involving doxxing received by the Office of PCPD

after the legislative amendment came into operation had increased by nearly seven times as compared with the past. More than 200 related complaints had been received since October 2021, and 70 complaints were received in January 2022 alone.

Implementation of section 33 of the Personal Data (Privacy) Ordinance

15. Some members expressed grave concern about the slow progress in bringing section 33 of PDPO into operation to regulate the transfer of data outside Hong Kong. PCPD advised that his Office had submitted recommendations to the Government in 2014 and remained in close communication with the Administration on the matter. The Administration explained that the implementation of section 33 could bring about significant and substantive impact on businesses. The Administration had commissioned a consultant to study the compliance measures that data users would have to adopt in order to fulfil the requirements under section 33.

16. At the meeting on 15 May 2017, the Panel received a briefing by the Administration on the preliminary findings of the business impact assessment on the implementation of section 33 of PDPO. Some members relayed the concerns expressed by the industrial and commercial sectors about the potential impacts of the implementation of section 33 of PDPO, especially on small and medium enterprises ("SMEs"), such as the high compliance cost that might be involved as a result of adopting measures to fulfil the requirements under section 33, as well as impacts on their operations and their online business.

17. The Administration advised that the consultant would first consolidate the final business impact assessment report, which was expected to be completed before the end of 2017. The representative of the Office of PCPD informed members that, upon receipt of the business impact assessment report, the Office of PCPD would study a number of issues relating to section 33 of PDPO, such as the Office of PCPD's mechanism for reviewing and updating the "white list" of jurisdictions with privacy protection standards comparable to that of Hong Kong, whether the industries already subject to stringent regulations could be regarded as having met the requirements of section 33 by means of compliance with the data protection requirements of their regulatory authorities, and the support measures required by SMEs to comply with the relevant requirements. The study would take at least a year's time to complete. The Administration advised that it would then formulate the steps forward in the light of the outcome of the Office of PDPO's study.

18. At the briefing by the former PCPD on 20 April 2020, members were informed that the Office of PCPD engaged a consultant in November 2018 to

provide specialist views on the implementation of section 33. The consultant recommended that the Office of PCPD should, amongst others, revise the recommended model clauses in the "Guidance on Personal Data Protection in Cross-border Data Transfer" ("the Guidance"), [2] in order to enhance practicability and user-friendliness of the Guidance and facilitate organizational data users, including SMEs, to directly adopt the relevant clauses in data transfer agreements according to their business needs. The Office of PCPD had engaged the consultant to also review the Guidance, including to update the recommended model clauses in the Guidance for industries' reference, and to revise the Guidance, including updating the recommended good practices for cross-border data transfer agreements for better protection of personal data.

Relevant Legislative Council questions

19. At the Council meetings of 27 January 2021 and 28 April 2021, Hon Elizabeth QUAT and Hon Martin LIAO raised a written and an oral question on protection of online personal data privacy respectively. The questions and the Administration's replies are at **Appendices 2** and **3** respectively.

Recent development

20. PCPD will brief the Panel on an update of the work of the Office of PCPD at the next meeting on16 May 2022.

Relevant papers

21. A list of relevant papers on the LegCo website is in **Appendix 4**.

Council Business Division 4
Legislative Council Secretariat
13 May 2022

[2] The Guidance was issued by the Office of PCPD in December 2014 to strengthen privacy protection for cross-border personal data transfer.

則行政長官可藉書面通知委任一人署理專員職位，直至(視情況所需)——*(由1999年第34號第3條修訂)*

(i) 新的專員根據第5(3)條獲委任為止；或

(ii) 專員回任為止。

(2) 根據第(1)款獲委任署理專員職位的人，在他獲委任的期間——

(a) 須執行專員在本條例下的職能；及

(b) 可行使專員在本條例下的權力。

(3) 第6條須適用於根據第(1)款獲委任署理專員職位的人，猶如該人是專員一樣。

(e) is for any other reason unable to perform the functions of his office,

then the Chief Executive may, by notice in writing, appoint a person to act as the Commissioner until, as the case requires— *(Amended 34 of 1999 s. 3)*

(i) a new Commissioner is appointed under section 5(3); or

(ii) the Commissioner resumes his office.

(2) A person appointed under subsection (1) to act as the Commissioner, whilst he is so appointed—

(a) shall perform the functions; and

(b) may exercise the powers,

of the Commissioner under this Ordinance.

(3) Section 6 shall apply to a person appointed under subsection (1) to act as the Commissioner as if that person were the Commissioner.

8. 專員的職能及權力

(1) 專員須——

(a) 就遵守本條例條文作出監察及監管；

(b) 促進及協助代表資料使用者的團體為第12條的施行擬備實務守則，以在遵守本條例條文(尤其是各保障資料原則)方面提供指引；

(c) 促進對本條例的條文(尤其是各保障資料原則)的認識及理解以及遵守；

(d) 對他認為可影響在個人資料方面的個人私隱的建議制定的法例(包括附屬法例)加以審核，並向建議制定該法例的人報告其審核結果；

(e) 進行視察，包括對屬政府部門或法定法團的資料使用者所使用的任何個人資料系統的視察；

8. Functions and powers of Commissioner

(1) The Commissioner shall—

(a) monitor and supervise compliance with the provisions of this Ordinance;

(b) promote and assist bodies representing data users to prepare, for the purposes of section 12, codes of practice for guidance in complying with the provisions of this Ordinance, in particular the data protection principles;

(c) promote awareness and understanding of, and compliance with, the provisions of this Ordinance, in particular the data protection principles;

(d) examine any proposed legislation (including subsidiary legislation) that the Commissioner considers may affect the privacy of individuals in relation to personal data

(f) 為更佳地執行他的其他職能而對資料處理及資訊科技進行研究及監察其發展，以顧及該等發展在個人資料方面對個人私隱相當可能有的不利影響；*(由2012年第18號第4條修訂)*

(g) 與——

(i) 在香港以外任何地方執行專員認為與其在本條例下的任何職能相似(不論全部或部分相似)的職能的人，進行聯絡及合作；及

(ii) 該等人士在某些相互關注的並涉及在個人資料方面的個人私隱的事項方面進行聯絡及合作；及

(h) 執行根據本條例或其他成文法則委予他的其他職能。

(2) 專員可作出所有為更佳地執行其職能而需要作出的或對此有助的所有事情，或為更佳地執行其職能而連帶須作出的所有事情，而在不影響前文的概括性原則下，專員尤可——

(a) 在認為任何類別的財產對——

(i) 為專員或任何訂明人員供給地方；或

(ii) 專員可執行的任何職能的執行，

屬必要時，取得及持有該財產，並可在持有該財產所按的條款及條件的規限下，處置該財產；

(b) 訂立、履行、轉讓、更改或撤銷任何合約、協議或其他義務，或接受他人所轉讓的合約、協議或其他義務；

(c) 承辦或執行合法信託，但限於以推動專員在本條例下須予執行或准予執行的職能為宗旨的信託及具有其他類似宗旨的信託；

(d) 接受饋贈及捐贈，不論是否受信託所規限的饋贈或捐贈；

and report the results of the examination to the person proposing the legislation;

(e) carry out inspections, including inspections of any personal data systems used by data users which are departments of the Government or statutory corporations;

(f) for the better performance of his other functions, undertake research into, and monitor developments in, the processing of data and information technology in order to take account of any likely adverse effects such developments may have on the privacy of individuals in relation to personal data; *(Amended 18 of 2012 s. 4)*

(g) liaise and co-operate with any person in any place outside Hong Kong—

(i) performing in that place any functions which, in the opinion of the Commissioner, are similar (whether in whole or in part) to any of the Commissioner's functions under this Ordinance; and

(ii) in respect of matters of mutual interest concerning the privacy of individuals in relation to personal data; and

(h) perform such other functions as are imposed on him under this Ordinance or any other enactment.

(2) The Commissioner may do all such things as are necessary for, or incidental or conducive to, the better performance of his functions and in particular but without prejudice to the generality of the foregoing, may—

(a) acquire and hold property of any description if in the opinion of the Commissioner such property is necessary for—

(e) 在獲得行政長官事先批准下，成為任何關注(不論是完全或部分)在個人資料方面的個人私隱的國際組織的正式成員或附屬成員；*(由1999年第34號第3條修訂)*

(ea) 進行推廣或教育活動或服務；及 *(由2012年第18號第4條增補)*

(f) 行使本條例或其他成文法則賦予他的其他權力。

(2A) 凡專員在執行其在本條例之下的職能的過程中，進行任何推廣或教育活動或服務，或提供任何推廣或教育刊物或材料，專員可為之徵收合理收費。 *(由2012年第18號第4條增補)*

(3) 專員在執行其職能或行使其權力時，可製備及簽立任何文件；凡任何與他執行職能或行使權力所合理附帶或相應引起的事宜，專員亦可在與該等事宜有關連的情況下，製備及簽立任何文件。

(4) 任何文件如看來是以專員的印章簽立的，須予接納為證據，在沒有相反證據的情況下須當作已妥為簽立。

(5) 為向資料使用者及資料當事人提供指引，專員可不時安排擬備不抵觸本條例的指引以顯示他擬執行其在本條例下任何職能或行使其在本條例下任何權力的方式，並安排將該指引藉憲報公告刊登。 *(由2012年第18號第4條修訂)*

(i) the accommodation of the Commissioner or of any prescribed officer; or

(ii) the performance of any function which the Commissioner may perform,

and, subject to the terms and conditions upon which such property is held, dispose of it;

(b) enter into, carry out, assign or accept the assignment of, vary or rescind, any contract, agreement or other obligation;

(c) undertake and execute any lawful trust which has as an object the furtherance of any function which the Commissioner is required or is permitted by this Ordinance to perform or any other similar object;

(d) accept gifts and donations, whether subject to any trust or not;

(e) with the prior approval of the Chief Executive, become a member of or affiliate to any international body concerned with (whether in whole or in part) the privacy of individuals in relation to personal data; *(Amended 34 of 1999 s. 3)*

(ea) carry out promotional or educational activities or services; and *(Added 18 of 2012 s. 4)*

(f) exercise such other powers as are conferred on him under this Ordinance or any other enactment.

(2A) The Commissioner may impose reasonable charges for any promotional or educational activities or services carried out, or any promotional or educational publications or materials made available, by the Commissioner in the course of the performance of the Commissioner's functions under this Ordinance. *(Added 18 of 2012 s. 4)*

(3) The Commissioner may make and execute any document in the performance of his functions or the exercise of his powers or in connection with any matter reasonably incidental to or consequential upon the performance of his functions or the exercise of his powers.

(4) Any document purporting to be executed under the seal of the Commissioner shall be admitted in evidence and shall, in the absence of evidence to the contrary, be deemed to have been duly executed.

(5) The Commissioner may from time to time cause to be prepared and published by notice in the Gazette, for the guidance of data users and data subjects, guidelines not inconsistent with this Ordinance, indicating the manner in which he proposes to perform any of his functions, or exercise any of his powers, under this Ordinance. *(Amended 18 of 2012 s. 4)*

9. 專員的職員等

(1) 專員可——

(a) 僱用他認為合適的人士(包括從事技術工作的人士及專業人士);及

(b) 以僱用以外的方法聘用他認為合適的從事技術工作的人士或專業人士,

以協助他執行其在本條例下的職能及行使其在本條例下的權力。

(2) 專員須——

(a) 釐定可根據第(1)(a)款僱用的任何人或任何屬於可根據該款僱用的某類別人士的人的薪酬及決定僱用該人的條款及條件;

9. Staff of Commissioner, etc.

(1) The Commissioner may—

(a) employ such persons (including technical and professional persons); and

(b) engage, other than by way of employment, such technical and professional persons,

as he thinks fit to assist him in the performance of his functions, and the exercise of his powers, under this Ordinance.

(2) The Commissioner shall determine—

(a) the remuneration and terms and conditions of employment of any person, or any person belonging to a class of persons, who may be employed under subsection (1)(a);

Press Releases

LCQ18: Protection of online privacy
****

Following is a question by the Hon Elizabeth Quat and a written reply by the Secretary for Constitutional and Mainland Affairs, Mr Erick Tsang Kwok-wai, in the Legislative Council today (January 27):

Question:

WhatsApp is a mobile application (the App) widely used by Hong Kong people for instant messaging. The App has recently issued a notice to its users requesting them to indicate whether they agree to the updated terms of service and privacy policy of the App (new terms), which include the following provision: the user agrees to share his/her user information with Facebook (FB), which is the owner of the App, and FB's subsidiaries. In the event that the user has not indicated his/her consent by the deadline, he/she will not be able to continue using the App. A large number of users of the App have criticised that the new terms undermine the protection for their privacy, and that the App's de facto forcing its users to accept the new terms is an abuse of its market power. Although the person-in-charge of the App has subsequently indicated that the new terms will only apply to business accounts and deferred the relevant deadline, the concerns of users are still not assuaged. On the other hand, the App's users in the United Kingdom (UK) and the European Union (EU) are not affected by the new terms for the time being. In this connection, will the Government inform this Council:

(1) whether it knows if the Office of the Privacy Commissioner for Personal Data (PCPD) has, upon review of the new terms, found the new terms to be in breach of the Personal Data (Privacy) Ordinance (Cap. 486) and related codes of practice/guidelines;

(2) given that the PCPD has written to FB and put forward some recommendations (including providing users who do not agree to the new terms with viable options that enable them to continue to use its service), whether it knows if the PCPD has received a reply; if the PCPD has, of the details;

(3) whether it has studied if the App's users in the UK and the EU not being affected by the new terms is attributable to the better protection provided by the privacy protection legislation in those places; if it has studied and the outcome is in the affirmative, whether it will, by making reference to such legislation, amend Cap. 486, in order to enhance the privacy protection for members of the public; if it will not, of the reasons for that and the alternatives available; and

(4) whether it knows if the PCPD has examined whether the messaging applications, social platforms and online media websites commonly used in Hong Kong have collected users' personal data excessively; if the PCPD has, of the details; if not, the reasons for that?

Reply:

President,

In response to the question raised by the Hon Elizabeth Quat, having consulted the Office of the Privacy Commissioner for Personal Data (PCPD), the response is as follows:

(1) and (2) Given the wide usage of the messaging application mentioned in the question by the general public in Hong Kong, and the keen concerns about the privacy issues arising from the new

terms on the sharing of personal data concerned, the PCPD has earlier sent a letter to that messaging application's United States headquarters, and maintained proactive communications with their representatives, while providing the following four suggestions:

- clearly explain to users the arrangements for the sharing of personal data under the new terms, and the personal data involved and the use of other data;

- delay the deadline of consideration by users, giving ample time for users to consider;

- since not all users using the messaging application have at the same time opened the social network accounts under question, it is therefore worthy to consider not to apply the new terms to those users; and

- consider providing to users who have not chosen to accept the new terms and privacy policy a workable plan to continue to use the messaging application.

Subsequently, the PCPD noted the company announced on January 15, 2021 that it had extended the deadline for users to accept its new terms of service and privacy policy from February 8 to May 15, and stated that it would provide further information and explanation to users within this timeframe.

The PCPD has earlier received the preliminary reply from the company; following on this, the PCPD will find out further details from the company, and request the company to provide more details to the public to alleviate public concerns. The PCPD will continue to pay close attention to the developments, so as to further assess whether the company has contravened the relevant requirements under the Personal Data (Privacy) Ordinance (PDPO).

(3) The PCPD is currently communicating with the representative from the company in a proactive manner. At this stage, the PCPD still does not have sufficient information to comment whether the United Kingdom and the European Union users are affected by the new terms, and whether this is relevant to those areas' respective privacy laws. That said, in light of the rapid development of the global privacy landscape (such as the implementation of the General Data Protection Regulation of the European Union), the PCPD will consider issuing guidelines on the personal data privacy problems of which the public should be aware when using social networks.

(4) Currently, the PCPD disseminates information from time to time, to explain to the public the privacy problems of which to be aware when using social networks, for example, the "Protecting Online Privacy - Be Smart on Social Networks" information leaflet (www.pcpd.org.hk//english/resources_centre/publications/files/SN2015_e.pdf). Moreover, upon receiving complaints and enquiries, the PCPD will review the collection, holding, processing, use or disclosure of personal data by relevant data users on online social networks, messaging applications, Internet media, etc., to ensure data users comply with the requirements of the PDPO and the Data Protection Principles. In future, the PCPD will strengthen the proactive patrolling work in this aspect, so as to further protect the privacy rights of the general public.

Ends/Wednesday, January 27, 2021
Issued at HKT 15:55

Press Releases

LCQ4: Protection of online personal data privacy
****

Following is a question by the Hon Martin Liao and a written reply by the Secretary for Constitutional and Mainland Affairs, Mr Erick Tsang Kwok-wai, in the Legislative Council today (April 28):

Question:

It has been reported that the personal data of some 500 million users worldwide of LinkedIn, an employment-oriented community networking platform, have recently been scraped and sold, and the social media platform Facebook was hacked last year, resulting in the personal data of its over 500 million users worldwide (of which nearly 3 million were Hong Kong people) being stolen and made public. The Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD) indicated earlier on that it had written to the operator of the former to seek clarifications, and to the operator of the latter to initiate a compliance check on the relevant incident. On the other hand, in recent years quite a number of people have engaged in online doxxing, i.e. making public on the internet (especially on social media) the personal data so obtained. In this connection, will the Government inform this Council:

(1) whether it knows (i) the progress made by the PCPD on its follow-up work/compliance check on the aforesaid two incidents, and (ii) the remedial measures taken by the operators concerned;

(2) whether it knows if the PCPD has assessed the effectiveness of the Guidance on Protecting Personal Data Privacy in the Use of Social Media and Instant Messaging Apps which the PCPD issued early this month, and what relevant public education and publicity activities that the PCPD has scheduled for the coming year (e.g. holding seminars);

(3) given that the PCPD refers personal data security incidents involving criminal elements (e.g. "access to computer with criminal or dishonest intent") to the Police for investigation, whether it knows if the PCPD will refer the aforesaid two incidents to the Police for investigation; as the two incidents reportedly involved acts of stealing data by hackers outside Hong Kong, how the PCPD and the Police deal with acts of infringements of Hong Kong residents' privacy by people outside Hong Kong; and

(4) given that the Government is currently working jointly with the PCPD on amending the Personal Data (Privacy) Ordinance (Cap. 486), including criminalising the acts of doxxing and empowering the Privacy Commissioner for Personal Data to undertake investigation and prosecution work in respect of doxxing incidents, of the related preliminary proposals?

Reply:

President,

In response to the question raised by the Hon Martin Liao, having consulted the Security Bureau and the Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD), the response is as follows:

(1) Upon the suspected personal data leakage incidents affecting the social media platform users of Facebook and LinkedIn, the PCPD immediately took an active lead in following up on the incidents, including initiating a compliance check against Facebook. The PCPD

also sent letters to remind the concerned social media platforms that if it was found that Hong Kong users were affected, they should notify the affected users as soon as possible to mitigate the possible risks arising from the incidents. According to the preliminary replies to the PCPD from the concerned social media platforms, Facebook responded that while investigations were ongoing, it was believed that the users' data was maliciously scraped from publicly accessible information on Facebook platforms before September 2019. To this end, Facebook provided an online contact form in its Help Centre for users to submit enquiries relating to the incident, including whether users' data had been improperly disclosed. LinkedIn responded to the PCPD that it was investigating the incident, and the disclosed personal data included publicly accessible information of members on the LinkedIn website, as well as information aggregated from other websites. The PCPD will continue to follow up on the above incidents.

(2) In April 2021, the PCPD issued the "Guidance on Protecting Personal Data Privacy in the Use of Social Media and Instant Messaging Apps" (Guidance), providing practical suggestions for the public to mitigate the privacy risks in the use of social media (www.pcpd.org.hk/english/resources_centre/publications/files/social_media_guidance.pdf). Such suggestions included matters the public should look out for when registering a new social media account, as well as how to manage privacy settings to limit the extent of disclosure of publicly accessible personal data. Upon issue, the Guidance has been widely reported by the media. Many media reports quoted the "Step-by-Step Guide on Adjusting Privacy Settings" in the Guidance, which advised the public on the means to strengthen the protection of privacy while using social media. In various media interviews, the PCPD also explained to the public the privacy risks associated with the use of social media and instant messaging software, and how to step up the protection of personal data privacy. Since its uploading to the PCPD website, the Guidance has gained over 2 200 views, and the PCPD has achieved 10 000 reaches when promoting the Guidance through various social media platforms. Besides, the PCPD has distributed the Guidance to the Home Affairs Enquiry Centres in all 18 districts for collection by members of the public. The Guidance has also been issued to various trade associations, professional bodies, public organisations and members of the PCPD Data Protection Officers' Club. for their reference. The PCPD has all along been undertaking various promotion, education and publicity activities to remind the public of the privacy risks involved in the use of social media and the mitigation measures. For example, in April 2021, the PCPD held an online seminar entitled "Protection of Personal Data Privacy in the Use of Information and Communications Technology". In the coming year, the PCPD will continue to organise related seminars and promotional activities, including an upcoming free public online seminar entitled "Social Media and You" in May, together with the production of promotional leaflets and videos to raise the public's vigilance in the protection of personal data privacy.

(3) Theft of personal data may not only contravene the Personal Data (Privacy) Ordinance (PDPO), but may also, depending on circumstances, breach other criminal offences, for example theft and obtaining property by deception offences under the Theft Ordinance (Cap. 210), access to computer with dishonest intent offence under the Crimes Ordinance (Cap. 200) etc. The PCPD is continuing to follow up on the above two suspected data leakage incidents. If there is evidence suggesting possible contravention of criminal offences, the case will be referred to the Police for follow up. As for cases involving outside-Hong-Kong elements, the Police will handle in accordance with powers granted under relevant existing laws in Hong Kong, for example the Criminal Jurisdiction Ordinance (Cap. 461).

(4) The Government attaches great importance to combating doxxing acts, which are intrusive to personal data privacy. To further

combat doxxing acts, the Government and the PCPD are working on the amendments to the PDPO. The directions of amendments mainly encompass: (1) criminalising doxxing acts as an offence under the PDPO, (2) conferring on the Privacy Commissioner for Personal Data (Commissioner) statutory powers to demand the removal of doxxing contents from social media platforms or websites, and (3) empowering the Commissioner to carry out criminal investigations and initiate prosecution. We aim to complete the drafting of the legislative amendments related to doxxing and submit the same to the Legislative Council for scrutiny within this legislative year.

Ends/Wednesday, April 28, 2021
Issued at HKT 17:16

NNNN

Appendix 4

Relevant documents on the Work of the Office of the Privacy Commissioner for Personal Data

Committee	Date of meeting	Paper
Panel on Constitutional Affairs	20.3.2017 (Item V)	Agenda Minutes
	15.5.2017 (Item IV)	Agenda Minutes
	14.2.2018 (Item IV)	Agenda Minutes
	18.3.2019 (Item IV)	Agenda Minutes
	20.4.2020 (Item V)	Agenda Minutes
	18.1.2021 (Item IV)	Agenda Minutes
Legislative Council	27.1.2021	Official Record of Proceedings Pages 107 to 110
	28.4.2021	Official Record of Proceedings Pages 17 to 20
Panel on Constitutional Affairs	18.10.2021 (Item II)	Agenda Minutes
	10.2.2022 (Item III)	Agenda

Council Business Division 4
Legislative Council Secretariat
13 May 2022