

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.