Privacy Commissioner's Opening Keynote Speech at

Data Privacy Forum

Thursday 22 April 2021; 9:15 am

Cyberport

1. Good morning, Jason (Jason Lau, chairperson of the conference), distinguished guests, ladies and gentlemen,

   I am very honoured to be invited to give an opening speech at this inaugural Data Privacy Forum.

Significant development in ICT

2. The rapid development of information and communications technologies (ICTs) in the past decade has completely changed our daily lives. If we call the period from around the middle of the eighteenth century to the middle of the nineteenth century the period of the Industrial Revolution, maybe we can call the past decade the beginning of the period of ICT Revolution. Nowadays, with the use of smart phones, social media, and e-commerce platforms, almost everything you need is at your fingertips.

Impact of COVID-19 on privacy risks

3. COVID-19 has further accelerated the digital transformation since last year. Owing to social distancing measures, many of us have to

work from home as well as do our marketing or shopping online. According to a study by McKinsey & Company in 2020[1], the digitalisation of customer interactions by organisations in the Asia Pacific has been accelerated by four years as a result of COVID-19.

ICT as a double-edged sword

4. However, the accelerated development of ICTs has also brought with it unprecedented yet non-negligible risks to personal data privacy. There is an old Chinese proverb, "Water can float a boat, so can it swallow the boat." Every click or tap that you made on your smart phone or computer may be recorded and analysed. The information which you provided to different platforms may be aggregated to produce big data for marketing purposes. Worse still, the information may end up in the hands of hackers.

5. In the past few weeks, for example, we saw users' data from several social media platforms improperly disclosed on some hackers' platforms. Over one billion user accounts worldwide were affected. This information, together with other publicly available information, when pieced together, can be used to profile the users for perpetuating frauds or other illegal purposes, including doxxing. Indeed, the biggest-ever phone scam case was just revealed in Hong Kong, involving a 90-year-old woman who allegedly lost HK$250

[1] McKinsey & Company, *How COVID-19 has pushed companies over the technology tipping point—and transformed business forever*, October 2020, accessible at: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

million, because the scammers were able to identify her by her full name, ID card number and phone number.

6. You may also remember that at around the same time last year, 'Zoombombing' happened when we started picking up the use of video conferencing software. In response, my Office joined force with five other data protection authorities in other parts of the world and we issued an open letter to the operators of major video conferencing companies in July last year, to remind them of their obligations to comply with data protection laws and handle users' personal data responsibly[2].

Stepping up personal data protection

7. Against this background, I must say the public's awareness of their personal data privacy is at an all-time high. Gone are the days when personal data protection was a mere compliance issue. It is indeed of paramount importance nowadays for organisations, i.e. data users, to protect and respect their customers' personal data in order to garner the trust of their customers and remain competitive in the market. It is becoming increasingly clear that a slip in one's privacy practice may lead to disastrous consequences, including losing a significant portion of your customers overnight. This is best

[2] PCPD media statement, 21 July 2020, accessible at: https://www.pcpd.org.hk/english/news_events/media_statements/press_20200721.html

illustrated by the recent saga relating to the change in the Terms of Service and Privacy Policy of a popular instant messaging app.

8. As part of the ICT Revolution, the protection of personal data privacy is apparently gaining importance on the agenda of some tech giants nowadays. For instance, a major smart phone brand now requires app developers to inform users of the categories of data collected from them by displaying a "nutrition label", and obtain users' consent before the developers conduct cross-platform tracking. Another tech giant which derives most of its revenue from online advertisement has vowed to phase out third-party cookies and introduce more privacy-friendly approaches for serving online advertisements. Hopefully, the tech giants will not shy away from assuming their social responsibilities and will join the privacy protection bandwagon to respect and protect their customers' privacy.

9. Indeed, I would appeal to all organisations to enhance their personal data privacy protection to cope with the rising expectations of their customers, and the public at large. Personal data protection should be a boardroom issue, with support and steer from the top. In practice, organisations should embrace personal data protection as part of their corporate governance responsibilities and implement it as a business imperative throughout the organisation. In this connection, the Privacy Management Programme (or in short, the PMP) advocated by my Office can be a useful tool. The PMP is a management framework that assists organisations in minimising

personal data privacy risks, as well as complying with the requirements of the Hong Kong privacy law, the Personal Data (Privacy) Ordinance (PDPO). I am pleased to inform you that the PMP has just been included in the Guide for Independent Non-Executive Directors recently published by the Hong Kong Institute of Directors as one of the drivers for the adoption of "Environmental, Social and Governance" (ESG) management.

10. Talking about PMP, the role of Data Protection Officers (DPOs) is indispensable. I believe that many of you are DPOs of your respective organisations. As DPOs, I would appeal for your support to ensure your respective organisations' compliance with the privacy law and the implementation of a PMP. Rather than sorting things out when a problem occurs, it is more important to incorporate Privacy by Design and Privacy by Default in the first instance in the development of new products and services. I believe that with a strong community of DPOs, we would be able to enhance data governance in your respective organisations and collectively build a privacy-friendly culture both in Hong Kong and in Asia.

Work of the PCPD

11. Turning to the work of my Office, the PCPD, I am very pleased to inform you that my Office, which was established in 1996, is

celebrating our 25th Anniversary this year, and we have plans to organize a series of events to mark this important milestone.

12. We kicked off the year with the inaugural Privacy-friendly Award, and altogether 100 organisations, both public and private, were awarded the Gold or Silver Certificates in recognition of their outstanding achievements in the protection of privacy in relation to personal data.
13. Looking ahead, we have several major projects coming up this year.

Doxxing

14. First and foremost, my Office is now working with the Government to formulate concrete legislative amendment proposals to tackle doxxing behaviour under our privacy law. As you may be aware, personal data has been weaponized in Hong Kong over the last two years. From June 2019 up to the end of last year, my Office handled over 5,000 doxxing-related complaints and cases discovered by us proactively through online patrols.
15. To quote the Chief Judge of Hong Kong in one of his judgments:

"*…The damage of widespread doxxing goes well beyond the victims. It seriously endangers our society as a whole. If doxxing practices are not curtailed, the fire of distrust, fear and hatred ignited by them*

will soon consume the public confidence in the law and order of the community, leading to disintegration of our society.[3]"

16. To more effectively combat doxxing, the Government's aim is to submit an amendment bill to our Legislative Council within this legislative session. Other amendment proposals to the PDPO, such as the introduction of administrative fines and a mandatory data breach notification system, will be dealt with separately.

Social Media

17. More recently, in the light of the widespread use of social media, my Office has published the "Guidance on Protecting Personal Data Privacy in the Use of Social Media and Instant Messaging Apps" earlier this month to provide some practical guidance to users on how to protect their personal data when they register for, and use, any social media. We will continue to publicise, or promote, the guidance with a view to raising the awareness of people when they navigate online.

Artificial Intelligence

18. Another priority for us this year is to work on issues relating to the protection of personal data in the development and use of artificial intelligence. A study by the Hong Kong Monetary Authority last year shows that 80% of the banks in Hong Kong have planned to

[3] *Junior Police Officer's Association v Electoral Affairs Commission & others* [2019] HKCA 1197, paragraph 19

increase investment in AI over the next 5 years[4]. Adoption of AI by other sectors is also picking up speed. However, if used improperly, AI poses significant risks to personal data privacy and other rights of individuals. It is high time that we should develop an ethical guidance for AI which incorporates internationally recognised principles and best practices. We are working in collaboration with the Office of the Government Chief Information Officer in this regard and it is our plan to produce a guidance note on the Ethical Development and Use of Artificial Intelligence around June this year.

International Collaboration

19. Lastly, as data sees no borders, we will continue to foster our collaboration with data protection authorities in other jurisdictions. Throughout the years, my Office has been an active member of the Global Privacy Assembly, which is an international forum for over 130 data protection authorities from around the world. In my capacity as the co-chair of the Working Group on Ethics and Data Protection in Artificial Intelligence set up by the Assembly, Hong Kong proposed, and sponsored the passage of, a Resolution on Accountability in the Development and Use of AI at the Assembly's annual conference last October. Among other things, the Resolution recommended 12 measures which might be adopted by

[4] Hong Kong Monetary Authority, *Report on "Artificial Intelligence in Banking: The Changing Landscape in Compliance and Supervision"*, 21 August 2020, accessible at: https://www.hkma.gov.hk/eng/news-and-media/press-releases/2020/08/20200821-3/

organisations for effectuating and demonstrating accountability in the development and use of AI, and I hope that the recommended measures would serve as an international benchmark for a robust accountability framework for the development and use of AI in future.

20. Further, to address privacy issues arising from the pandemic, we would continue our work as a member of the Assembly's COVID-19 Working Group. We spearheaded the compilation of a Compendium of Best Practices in Response to COVID-19 last year, covering areas such as contact tracing and the sharing of health data. This year, we plan to produce another Compendium to set out the international best practices in areas such as health passports and the keeping and sharing of vaccination records.

Closing

21. To conclude, I am sure that if we work together, we can rebound with greater strength after the pandemic, and we can build a stronger global community for the better protection of data privacy.
22. May I wish you all a very fruitful and inspiring conference.
23. Thank you.