PCPD's Submission to the OHCHR to Provide Inputs to a Report on "The Right to Privacy in the Digital Age"

This submission is made by the office of the Privacy Commissioner for Personal Data, Hong Kong, China (**PCPD**) to the Office of the United Nations High Commissioner for Human Rights (**OHCHR**), in response to the OHCHR's call for inputs to a report on "the right to privacy in the digital age"[1].

Privacy Protection in Hong Kong, China

2. The International Covenant on Civil and Political Rights (**ICCPR**) has been applied to Hong Kong since 1976. In 1991, the Hong Kong Bill of Rights Ordinance (Cap 383, Laws of Hong Kong) came into force mirror-imaging the provisions of the ICCPR[2]. In 1995, the Personal Data (Privacy) Ordinance (Cap 486, Laws of Hong Kong; **PDPO**[3]), which was modelled on the OECD Privacy Guidelines 1980 and the Data Protection Directive 1995 of the then European Communities, was enacted to regulate the processing of personal data and protect personal data privacy. The PDPO is a comprehensive data protection law applicable to both the private and public (i.e. government) sectors.

3. The Basic Law[4], which is the constitutional document of Hong Kong, also guarantees a host of rights to Hong Kong residents. For example, Article 30 of the Basic Law provides constitutional guarantee for freedom and privacy of communication[5].

[1] http://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportPrivacy.aspx
[2] Section 8 of the Hong Kong Bill of Rights Ordinance (Cap 383): https://www.elegislation.gov.hk/hk/cap383
[3] Personal Data (Privacy) Ordinance (Cap 486): https://www.elegislation.gov.hk/hk/cap486
[4] The Basic Law came into operation on 1 July 1997 when the People's Republic of China resumed its exercise of sovereignty over Hong Kong (which then became a Special Administrative Region of China).
[5] Chapter III of the Basic Law – Fundamental Rights and Duties of the Residents: http://www.basiclaw.gov.hk/en/basiclawtext/chapter_3.html

4. The PDPO has undergone a significant revamp in 2012. In particular, the penalties for improper use of personal data in direct marketing were heightened[6]; a new offence for disclosing personal data obtained without consent from data users was introduced[7]. The amendments also empower the PCPD to grant legal assistance to an aggrieved individuals seeking compensation from a data user for damages suffered as a result of the data user's breach of the PDPO[8].

5. In October 2017, the High Court of Hong Kong handed down a judgement on a judicial review application[9] concerning the scope and constitutionality of section 50(6) of the Police Force Ordinance (Cap 232, Laws of Hong Kong; **PFO**) in relation to the search of the digital contents of seized mobile phones[10]. In the judgment, the High Court declared that on a proper construction of section 50(6) of the PFO, a police officer is authorised to search the digital content of a mobile phone (or a similar device) seized upon arrest *without warrant only in exigent circumstances*, i.e.: when a person has been lawfully arrested under section 50, and the police officer reasonably suspects such an urgent search may:-

a. prevent an imminent threat to safety of the public or police officers;
b. prevent imminent loss or destruction of evidence; and

[6] Sections 35A to 35M of the PDPO
[7] Section 64 of the PDPO
[8] Section 66B of the PDPO
[9] *Sam Wing Kan v Commissioner of Police*, HCAL 122/2014: http://legalref.judiciary.hk/lrs/common/search/search_result_detail_frame.jsp?DIS=111978&QS=%2B&TP=JU&ILAN=en
[10] Police Force Ordinance (Cap 232), section 50(6) (https://www.elegislation.gov.hk/hk/cap232):
"*Where any person is apprehended by a police officer it shall be lawful for such officer to search for and take possession of any newspaper, book or other document or any portion or extract therefrom and any other article or chattel which may be found on his person or in or about the place at which he has been apprehended and which the said officer may reasonably suspect to be of value (whether by itself or together with anything else) to the investigation of any offence that the person has committed or is reasonably suspected of having committed…*"

c. lead to the discovery of evidence in extremely urgent and vulnerable situation[11].

6. The High Court also noted that nowadays mobile phone is akin to a personal computer where massive and extensive personal data and information can be stored in and accessed through it. Hence, such contents shall be subject to significant and high privacy protection constitutionally[12].

Challenges in the Digital Age and Recommended Good Practice

7. Innovative technologies such as big data analytics, Internet of Things (**IoT**), machine learning and artificial intelligence unleash the value of data, drive economic growth and improve our well-being. Unavoidably, they also cause privacy concerns. Improper use of personal data may even deprive individuals of their other interests and freedoms.

8. Although the PDPO, like many other data protections laws, is principle-based and technology neutral, new information and communication technologies (**ICTs**) are stretching the limits of some fundamental principles of personal data protection, such as data minimisation, transparency and use limitation. For example, the ubiquity of data collection and the unpredictability of data use make it very difficult, if not impossible, to provide individuals with meaningful notice; strict enforcement of use limitation principle may well prevent personal data from being used in the advancement of public interests. This is especially the case when the PDPO legislative reform in 2012 mentioned earlier did not address such privacy concerns in the digital age.

9. Therefore, since 2014, the PCPD has been encouraging organisations to make a paradigm shift from compliance to accountability by implementing the

[11] Paragraph 64 of the judgement
[12] Paragraph 23 of the judgement

Privacy Management Programme (**PMP**)[13]. The PMP should be a robust privacy infrastructure that:-

a. has top management commitment and is integrated into the organisation's governance structure;
b. establishes policies and procedures giving effect to the requirements under the PDPO;
c. provides for appropriate safeguards based on privacy risk assessment;
d. includes plans for responding to breach and incident; and
e. incorporates internal oversight and review mechanisms.

10. In addition to ensuring legal compliance, the PMP demonstrates an organisation's commitment to good corporate governance and is conducive to building trustful relationships with customers, employees, shareholders and regulators.

11. Apart from the PMP, the PCPD has issued a few publications[14] last year to promote good practice in the use of ICTs, such as IoT and big data analytics. Bearing in mind the principles of accountability, the publications made the following recommendations to organisations intending to use these ICTs:

a. be transparent;
b. adopt privacy by design and privacy by default; and
c. respect individuals' interests, rights and freedoms.

12. The adoption of accountability or the PMP is currently voluntary in Hong Kong. The PCPD is reviewing whether to make accountability

[13] PCPD's Privacy Management Programme: https://www.pcpd.org.hk/pmp/pmp.html
[14] E.g.: "*2016 Study Report on The Privacy Policy Transparency of Fitness Bands*" (January 2017): https://www.pcpd.org.hk/english/news_events/media_statements/press_20170124.html; "*Physical Tracking and Monitoring Through Electronic Devices*" Information Leaflet (May 2017): https://www.pcpd.org.hk/english/news_events/media_statements/press_20170511.html; "*2017 Study Report on User Control over Personal Data in Customer Loyalty and Reward Programmes*" (December 2017): https://www.pcpd.org.hk/english/news_events/media_statements/press_20171218.html

mandatory under the law, requiring organisations to take the initiative in personal data protection and therefore, nipping privacy risks in the bud.

Biometric data

13. The PCPD also noticed the increasing use of biometric data, mainly for security purpose. Biometric data like fingerprints, facial images, retinal images is an effective and convenient tool for user identification and authentication because of its uniqueness and accuracy. However, because of its uniqueness, accuracy and (for some kinds of biometric data like fingerprints) immutability, a breach of biometric data may lead to high risk of impersonation and other abusive uses, which may be incurable (e.g., one cannot change his fingerprints even the data is breached). Some biometric data may even be able to expose intimate information about a person, such as ethnic origins, health conditions and sexual orientation. Improper use of biometric data may lead to unfair discrimination, among other possible harms.

14. Having considered the risks of processing biometric data, the PCPD issued a guidance in 2015, setting out our expectations on the collection, use and processing of biometric data[15], which include:

a. conducting privacy impact assessment before collection of biometric data, and always opting for the least privacy-intrusive alternative whenever possible;
b. minimising the extent of collection of biometric data;
c. providing individuals with free and informed choices; and
d. establishing strong controls for access to, use and transfer of biometric data.

[15] "Guidance on Collection and Use of Biometric Data" (July 2015): https://www.pcpd.org.hk//english/resources_centre/publications/files/GN_biometric_e.pdf

15. The PDPO, as it now stands, does not contain provisions differentiating sensitive personal data from other kinds of personal data. However, it is indisputable that some kinds of personal data, like biometric data, are more sensitive and thereby warranting greater protection. The PCPD is reviewing whether to make explicit provisions in the law to set out the kinds of personal data that are sensitive, and the additional safeguards required for processing of this sensitive data.

Anonymisation and Encryption

16. Anonymisation and encryption are two useful tools to protect personal data privacy. The PCPD reckons that anonymisation, if properly implemented, may be an alternative to data erasure, and the anonymised data may be used for other purposes, like research and statistics[16]. The PCPD also encourages organisations to encrypt personal data in transit and in storage to protect the data from unauthorised access[17].

17. However, to date, there is no internationally accepted standard for anonymisation or de-identification (the ISO 20889 – "*Privacy enhancing data de-identification techniques*" is still under development[18]). This may create uncertainty to the quality of anonymisation works. Improvement in techniques of data mining, data analytics and profiling increases the risk of re-identification further. Indeed, there were numerous incidents in which individuals had been re-identified from de-identified information.

18. Similarly, incorrect use of encryption algorithms may render the encrypted data susceptible to cracking or decoding by unauthorised parties and

[16] See PCPD's "*Guidance on Personal Data Erasure and Anonymisation*" (April 2014), page 4: https://www.pcpd.org.hk//english/resources_centre/publications/files/erasure_e.pdf
[17] See PCPD's "*Guidance for Data Users on the Collection and Use of Personal Data through the Internet*" (April 2014), page 4: https://www.pcpd.org.hk/english/publications/files/guidance_internet_e.pdf
[18] https://www.iso.org/standard/69373.html

therefore, leaking sensitive information. Advancement in computing powers may render once strong encryption algorithms vulnerable.

19. Hence, while the value of anonymisation and encryption is acknowledged, it is important to remind data users/controllers that anonymisation or encryption alone may well not suffice for giving adequate protection to personal data. In fact, in a recent investigation, the PCPD found a government department in breach of the data security requirement under the PDPO due to the loss of a notebook computer containing personal data, despite the government department had assured the PCPD that multiple layers of encryption had been applied to the data concerned[19]. Data users/controllers should also adopt other organisational measures like conducting risk assessments and putting in place relevant safeguards to prevent the anonymised data and encrypted data from unauthorised access.

Government Surveillance Activities

20. Law enforcement agencies may have genuine needs to conduct surveillance activities for prevention and investigation of crimes and protection of public security. The Interception of Communications and Surveillance Ordinance (Cap 589, Laws of Hong Kong; **ICSO**) was enacted in 2006 (and revised in 2016) to regulate the conduct of interception of communications and the use of surveillance devices by law enforcement agencies[20]. A law enforcement agency is prohibited from carrying out any *interception* of communications (transmitted by a postal service or a telecommunications system[21]) or *covert* surveillance[22] without prescribed authorisation[23], in most

[19] https://www.pcpd.org.hk/english/news_events/media_statements/press_20170612.html
[20] The Interception of Communications and Surveillance Ordinance (Cap 589): https://www.elegislation.gov.hk/hk/cap589
[21] Sections 2 and 4 of the ICSO
[22] Section 5 of the ICSO
[23] Sections 4 and 5 of the ICSO

cases by a judge[24]. An independent oversight authority, the Commissioner on Interception of Communications and Surveillance, has been established to oversee compliance by the law enforcement agencies with the requirements under the ICSO[25].

21. There are views that the ICSO does not keep up with technological developments and changes in the modes of communications of the general public[26]. For example, user data and stored communications including social media and instant messaging are not covered by the ICSO. In the circumstances, wiretapping may no longer be necessary, and information stored on the servers of online services providers may be obtained by a law enforcement agency without prescribed authorisation. Hence, there are calls for changes to the law in order to afford more protection to the privacy of communications.

22. Under section 58 of the PDPO, personal data may be used (including disclosure) for prevention or detection of crimes, or apprehension, prosecution or detention of offenders, among other things, without data subjects' consent, provided that the operation of the consent requirement would be likely to prejudice these law enforcement actions. Pursuant to section 58 of the PDPO, a balance may be struck between legitimate government surveillance activities and personal data privacy protection. However, because law enforcement agencies may withhold information in relation to their investigations when making data access requests to business operators, and those business operators may generally lack the information and resources to verify whether the data access requests are valid or whether the requests have passed the prejudice test under section 58 of the PDPO, business operators tend to "cooperate" with the law enforcement agencies when such requests are made to them, and disclose the relevant data (including personal data) to the law enforcement agencies.

---

[24] See Summary of the Annual Report 2016 of the Commissioner on Interception of Communications and Surveillance, paragraph 3: http://www.sciocs.gov.hk/en/pdf/Annual_Report_2016_Summary.pdf
[25] Section 39 of the ICSO
[26] "*Hong Kong's communications interception law should be updated to protect privacy*" (18 December 2017): http://transparency.jmsc.hku.hk/?p=2453

23. Potential measures to improve the check and balance on government surveillance activities in Hong Kong may include:

a. setting out more detailed guidance or code of practice to law enforcement agencies on inspection of communications;
b. expanding the scope of the ICSO to require prescribed authorisation for inspection of stored communications and the corresponding metadata by law enforcement agencies; and/or
c. expanding the definition of "personal data" under the PDPO to explicitly include stored communications and metadata as long as they relate to an identified or identifiable individual.

Concluding Remarks

24. The PCPD fully appreciates the importance of protecting privacy as a fundamental human right and recognises the challenges to privacy protection in the digital age. However, the PCPD would like to stress that privacy protection is a balancing exercise, in which the rights, interests and freedoms of all stakeholders (including individuals, businesses, governments, regulators and the general public, where appropriate) should be taken into account. That said, given the power imparity between individuals and institutional data users/controllers, proper regulations and mechanisms should be put in place to hold the latter accountable for their collection, processing and use of personal data. At the same time, proper tools should be developed to assist data users/controllers to give effect to the spirit of the privacy/data protection regulations. The international communities, including the OHCHR, are expected to play a significant role in developing international standards for these regulations, mechanisms and tools, and thereby strengthening the right to privacy as a global fundamental human right.

Privacy Commissioner for Personal Data, Hong Kong, China
April 2018