

Global Privacy Forum

Data Protection and Privacy Implementation, Compliance, and Initiatives from the East

4 December 2019, Cebu, Philippines

Stephen Kai-yi WONG, Barrister
Privacy Commissioner for Personal Data,
Hong Kong, China

Personal Data Privacy Challenges in the Digital Age

2

(1) Excessive collection of personal data

67.2% respondents
think smartphone APPs
collect unnecessary
personal information



What data do APPs ask permissions for?



Source: China Consumers' Association 'Report on Personal Data Leakage from APPs' (August 2018)

Apps used “dark patterns” to discourage users from exercising their privacy rights:

Turn on face recognition if you want us to use this technology

If you turn this setting on, we'll use face recognition technology to understand when you might appear in photos, videos and the camera to do things such as help protect you from strangers using your photo, find and show you photos that you're in but haven't been tagged in, tell people with visual impairments who's in a photo or video, and suggest people that you may want to tag. Select Accept and Continue to turn on face recognition or Manage Data Settings to keep it turned off.

What's collected?

MANAGE DATA SETTINGS

ACCEPT AND CONTINUE

- Making the least privacy-friendly settings as the default settings
- Making the alternative privacy settings difficult to navigate
- Using eye-catching buttons for less privacy-friendly options
- Emphasize the positive aspects of less privacy-friendly options, glossing over potential privacy risks
- Falsely claim that not accepting the default option would affect the functionality

Help Support Wordscapes

The developers of Wordscapes need the help of our community. We can make content that you enjoy because of the revenue we generate on advertising.

You can help us make the ad experience more relevant by agreeing to share Personal Information such as device identifiers, IP address, demographics, and interest data about you. See [details](#) for more information.

Accept & Continue

(2) Covert collection of personal data

Beware of hackers when using spy cameras at home, Hong Kong's consumer watchdog warns

Sensitive images could be published online if basic security steps are not taken



Harminder Singh
Published: 6:45pm, 15 Mar, 2017



- ❑ Home surveillance cameras have become popular with consumers looking to keep an eye on their homes, children, or pets while they are away.
- ❑ Users can log in from anywhere in the world.
- ❑ Vulnerable to hacking
- ❑ Back doors in the software of IP cameras that will lead to recordings or image leaks.

5

Source: <https://www.scmp.com/news/hong-kong/education-community/article/2079135/beware-hackers-when-using-spy-cameras-home-hong>

(3) Increased outsourcing of data processing

More data collected in the digital age, more needs for outsourcing data processing

There may be unknown/little control over data storage locations

Outsourcing arrangements may be rapidly changing or loose

Amplifying privacy and security risks

Data processors not directly regulated by the PDPO

Problematic for:
Data retention
Data security

(4) Profiling and Re-identification

- Advancement in technology making re-identification of **anonymised dataset possible**, e.g blurred images captured by CCTV which contain unique facial features and medical records
- By **linking unencrypted parts** of the records with **publicly known information**, anonymised personal data can be re-identified.



Source: <https://www.gettyimages.hk/>

(5) Increased number of data breach incidents due to cybercrime or human errors – some examples in Hong Kong:

South China Morning Post

Law and Crime

Personal data of some 380,000 Hong Kong broadband customers hacked, service provider says

Hong Kong Broadband Network, the city's second largest fixed-line residential broadband provider, discovered on Monday that an inactive customer database had been accessed without authorisation

 **Danny Mok**
Published: 7:47pm, 18 Apr, 2018

South China Morning Post

Transport

Personal data of 9.4 million passengers of Cathay Pacific and subsidiary leaked, airlines say

- Information consists of passengers' names, nationalities, dates of birth, identity card numbers and historical travel details
- Suspicious activity detected in March, prompting a cybersecurity investigation – but IT lawmaker questions why carrier waited till now to disclose breach

Hong Kong economy

Credit reporting agency TransUnion forced to suspend online services over personal data security flaw as Hong Kong leader urges fix

- Chief Executive Carrie Lam was among those affected by easy online authentication procedures
- TransUnion, which compiles credit reports for banks and lending institutions, handles the data of 5.4 million consumers in Hong Kong

 **Denise Tsang**
Published: 7:15pm, 29 Nov, 2018

Source: SCMP (29 Nov 2018; 18 Apr 2018), HKFP (9 Apr 2019)



Possible reforms of the Personal Data (Privacy) Ordinance to align with international regulatory standards and to cope with the digital challenges

Possible amendments to PDPO :

(1) Expand the definition of 'personal data' under PDPO:

Personal data may include:

- Information practicable to ***ascertain an identity*** (direct/indirect); and
- Information ***relating to an identifiable*** person

Definitions of “personal data”

PDPO	Overseas (e.g. AU, CA, EU)
Criteria: • Practicable to <u>ascertain identity</u>	Criteria: • Relating to or about an <u>identifiable</u> individual
Meaning: • <u>Knowing</u> who a person is	Meaning: • Able to <u>single out</u> a person, not necessarily knowing who the person is
Result: • <u>Narrower</u> scope of personal data and <u>less</u> protection to privacy	Result: • <u>Wider</u> scope of personal data and <u>stronger</u> protection to privacy

Possible amendments to PDPO (cont.)

(2) Additional regulation on the retention of personal data

- Disclose personal data **retention policy**
- Stipulation of **maximum retention period**

Possible amendments to PDPO (cont.)

(3) Regulate data processors directly

Data processors' obligations on:

- **retention period** of personal data
- **security** of personal data
- **notification to data users** of data breaches without undue delay
- Data processors with a Hong Kong link or a presence in Hong Kong will be covered.

13

Possible amendments to PDPO (cont.)

(4) Mandatory Breach Notification

- Notify both the **PCPD** and the **impacted individuals**
- High threshold for breach notification – “*real risk of significant harm*” to individuals
- Set **time limit** – e.g. 5 days for notifying PCPD; ‘as soon as practicable’ for notifying individuals
- Allow for investigation period for ‘suspected breach’ before notification

Possible amendments to PDPO (cont.)

(5) Accountability Principle

- Include accountability principle in PDPO

HKMA'S CIRCULAR ON 3 MAY 2019



- To all authorized institutions
- Expressing support to PCPD's concept of data ethics and stewardship
- Encouraging adoption of PCPD's Ethical Accountability Framework in development of Fintech in order to-
 - Address privacy concerns of customers
 - Enhance customers' trust in using Fintech

<https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190503e1.pdf>

16

HKMA's circular on 5 November 2019



HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref: B1/15C
B9/67C

5 November 2019

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence by Authorized Institutions

I am writing to provide authorized institutions (“AIs”) with a set of guiding principles on consumer protection aspects in respect of the use of big data analytics and artificial intelligence (“BDAI”).

...

4. Data privacy and protection

...

(a) if personal data are collected and processed by BDAI applications:

...

- pay regard to the relevant good practices issued by the PCPD related to BDAI and Fintech, including, among others, the “Ethical Accountability Framework” (the “Framework”), the “Data Stewardship Accountability, Data Impact Assessments and Oversight Models” in support of the Framework, and the “Information Leaflet on Fintech”;

...

Possible amendments to PDPO (cont.)

(6) PCPD's Powers

Confer additional powers on the PCPD to:

- Conduct **criminal investigations/prosecutions**
- Impose **administrative fines**
- Make **prohibitive orders by way of interim enforcement notices binding on any relevant parties**

Recent 'Doxxing' in Hong Kong

- Privacy intrusive/intimidating messages and posts spreading at an alarming rate
- Weaponization of Personal Data
- From 14 June to 22 November 2019, the PCPD
 - Received and found **4,666** cases
 - Written **129** times to **15** platforms to request deletion (**1,631** links were removed)
 - **1,299** cases have been referred to the Police for investigation



Possible regulatory response to doxxing

- ❖ Give the PCPD powers to conduct **criminal investigation** and **prosecution of criminal offences**
- ❖ Allow PCPD to **apply to court for injunction** stopping doxxing
- ❖ Expanding the scope of protection to include platforms and webpages that have **close connection to Hong Kong** (the “**Hong Kong Link**”)
- ❖ Give the PCPD powers to **directly issue prohibitive orders by way of interim enforcement notices** to relevant social media platforms and website (e.g. take down doxxing posts, provide personal data of those posting doxxing messages)

20

Fragmentation of International Regulatory Standards

- Lack of global interoperable standards
- Bring challenges to the operation of multinational corporations → more costs on compliance
- Impede Fintech growth
- Restrictions on cross-border data flow and innovative use of data
- International collaborations to be promoted

Developments toward Interoperability and the Importance of Increasing Convergence

- Data Protection Authorities to develop a bilateral or multilateral assistance mechanism
- Regional harmonisation can provide legal certainty
- Adopting an internationally accepted standard or certification such as ISO27701, the world's first international standard for managing privacy information
- Increasing convergence can facilitate cross-border data transfer and reduce friction for multinational companies' operations
- Facilitate continued growth of technologies

22

Contact Us



Copyright



☐ Hotline

+852 2827 2827

☐ Fax

+852 2877 7026

☐ Website

www.pcpd.org.hk

☐ E-mail

enquiry@pcpd.org.hk

☐ Address

1303, 13/F, Sunlight Tower,
248 Queen's Road East,
Wanchai, Hong Kong, China

This PowerPoint is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this PowerPoint, as long as you attribute the work to the Office of the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0.

23