

53rd Asia Pacific Privacy Authorities Forum

Personal Data Protection Issues arising from COVID-19 in Hong Kong, China

3 June 2020 (Virtual meeting)

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





Data-led Measures to combat COVID-19 pandemic

(1) Electronic wristbands + mobile app

- Electronic wristbands paired with a mobile app – *StayHomeSafe* – to enforce home quarantine
- Currently mandatory for all people coming to HK

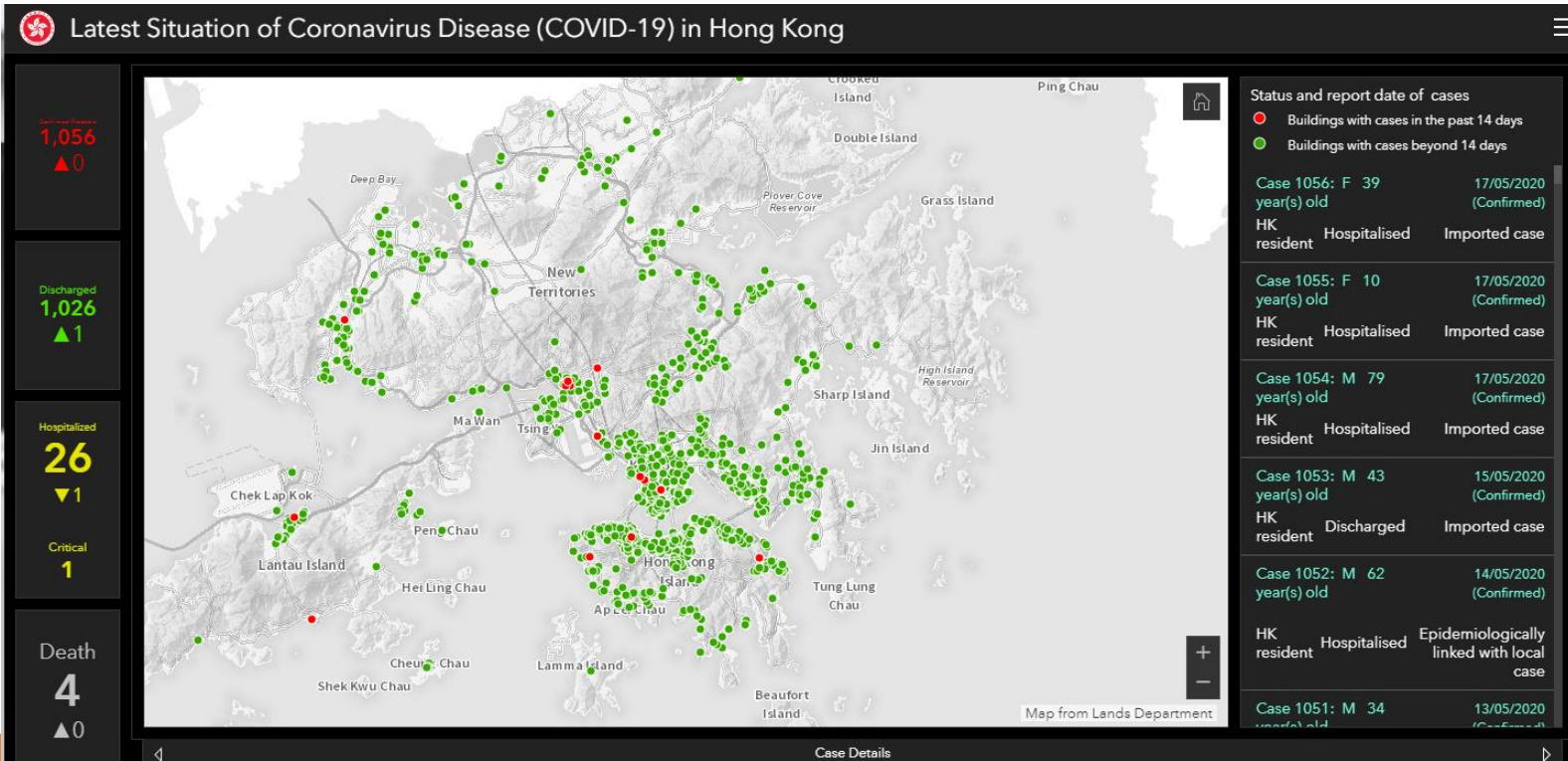


(1) Electronic wristbands + mobile app

- Wristbands do not contain GPS device
- Mobile app does not collect geo-location data
- Confirm a person is staying at home by analysing environmental communication signals such as Bluetooth, Wi-Fi and geospatial signals



(2) Online dashboard



Source: <https://chp-dashboard.geodata.gov.hk/covid-19/en.html>

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

(2) Online dashboard

- Lists out the buildings and vessels in which the confirmed or probable infection cases have resided/ taken
- Gender and age of patients disclosed
- Does not contain data that is precise enough to identify the infected person
- Well-balanced between privacy and information transparency

(3) Other contact tracing & exposure notification measures

- Verbal inquiry for contact tracing
- Supercomputer and big data analytics to identify close contacts
- Considered using location data (such as the route of a confirmed patient during a particular transport trip) collected by mobile operators to locate people in the vicinity of patients



Exemptions under data protection law

- Exemptions under the Personal Data (Privacy) Ordinance for using identity and location data:
 - Section 59 – protection of health
 - Section 60B – authorisation by law, i.e. Prevention and Control of Disease (Disclosure of Information) Regulation



(4) Octopus & The University of Hong Kong Research Initiative to combat COVID-19

- Using aggregate statistical data about usage of Octopus card to track the transmission of virus and identify the risk of infection in various districts, including information about the contact pattern and intensity of Hong Kong residents in different areas



Press Release

Octopus to Assist The University of Hong Kong in Research Projects to Contain the Spread of the COVID-19

(Hong Kong, 2 April 2020) – The LKS Faculty of Medicine, The University of Hong Kong (HKUMed) and Octopus Cards Limited (OCL) today jointly announced that due to the severity of the COVID-19 pandemic, OCL has, on the request by HKUMed, agreed to provide aggregate statistical data relating to the usage of Octopus cards for the purpose of supporting HKUMed to conduct research projects to contain the continuous spread of COVID-19 in Hong Kong.

The relevant information to be provided to HKUMed is of aggregate value, incapable of ascertaining the identity of any individual person and the usage data of a particular Octopus card, and is not "personal data" as defined in the Personal Data (Privacy) Ordinance (Ordinance). The aggregate data contains no name, no personal identification number, no phone number, no email address, no card identifier and no account number. The relevant information pertains to the usage of Octopus cards for the period from 1 January 2020 until the pandemic is declared over by the HKSAR Government.

HKUMed has undertaken with OCL that the relevant information provided is strictly for the purpose of conducting the said research projects in the effort to curb the COVID-19 spread, and will not be used, whether in whole or in part, for any other purposes or in any manner whatsoever without the prior written consent of OCL.

9

Source: Octopus Holdings Limited

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

PCPD



PCPD.org.hk

HK

(4) Octopus & The University of Hong Kong Research Initiative

- Does not contain names, personal identification numbers, phone numbers, card identifiers, etc.
- Data incapable of ascertaining the identity of any individual person



10

(5) Other relief & prevention measures

- Distribution of reusable masks
- Cash pay-out scheme
- Employment support scheme
- Closing of bars, karaoke etc.
- Restriction of gatherings and catering seating



Source: <https://www.qmask.gov.hk/>

11



The Regulator's Stance towards collection and use of personal data during the pandemic

PCPD's views on these measures

- “Right to life” should always be of paramount concern and privacy right is secondary to the right to life
- Legitimate and proportionate for the Government to collect and use personal data of the patients, confinees and their close contacts with a view to ensuring public health and safety
- Data protection laws are not an obstacle in the battle against the pandemic

Proportionality test passed!



- Is there a **pressing need** for such measures (e.g. pandemic and short of compulsory quarantine vacancies)?
- Would these measures serve the **legitimate purposes** of controlling and preventing the spread of coronavirus and saving lives of the public?
- Is there a **rational connection** between these measures and the legitimate purposes?
- Are these measures **no more than necessary** to achieve the legitimate purposes?
- Are the benefits of achieving the legitimate purposes **not disproportionate to the encroachment and inroads made into the fundamental right of personal data privacy**, i.e. not imposing an unacceptable harsh burden on the affected individuals?

Be a Protector and Facilitator

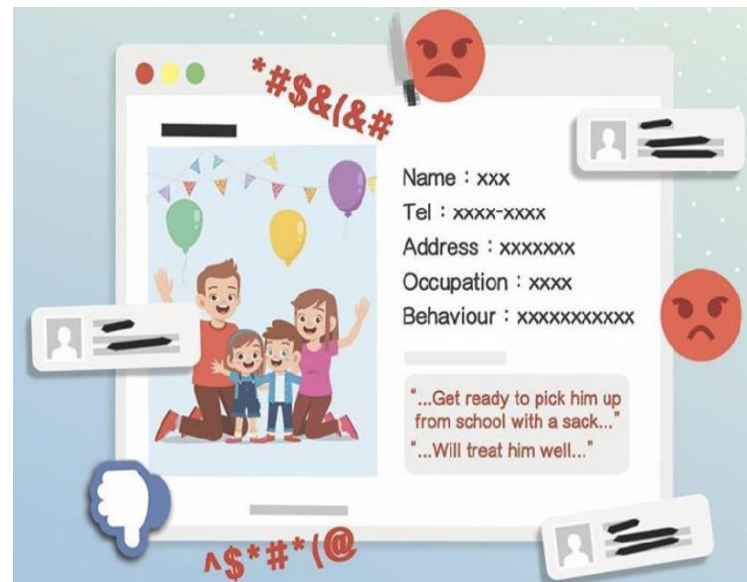
- Pragmatic approach has been adopted with the emphasis on the importance of **transparency** and **explainability**
- Less privacy-intrusive measures such as using anonymous data should always be preferred
- Exemptions under the PDPO may be applicable if necessary to protect public health



Other undesirable issues arising from COVID-19

(1) Doxxing

- Doxxing of medical workers who went on strike in early-2020
- Unlawful disclosure of their family members' personal data
- Prima facie case of contravention of a criminal offence under section 64(2) of the PDPO, subject to a maximum fine of HK\$1,000,000(or US\$128,900) and imprisonment for 5 years



(1) Doxxing

- Received/found 78 cases involving 4 online platforms and 17 web links (as at 15 May2020)
- PCPD urged website operators to remove/delete the posts/content
- Liaised with overseas data protection authorities to cover platforms outside HK

(2) Excessive collection and misuse of personal data

- Received 56 complaints of excessive data collection during organizations'/ shops' handing out/selling of daily necessities (as at 22 May 2020)
- Data should only be collected while necessary and data subjects shall be notified of the purpose and use
- PCPD urged the public to be vigilant, and organisations to comply with the PDPO during collection, usage, and retention of personal data

(3) Security issues of videoconferencing app

- Zoom bombing
- No end-to-end encryption
- Insecure cloud storage



(3) Privacy/ Security by design

- Can save subsequent hassles
- Transparency and explainability to gain trust
- PCPD issued privacy tips via social media and press release

13 Privacy Tips for Online Teaching and Video-conferencing

For Teachers and Conference Hosts

Before online teaching / video-conferencing

- 1. Take security measures**
Install the latest version of the programme, anti-virus software and firewalls; conduct privacy impact assessment
- 2. Guard the gate**
As a "gatekeeper", use the virtual "Waiting Room" to conduct "mandatory quarantine" to verify the participants' identity before the meeting so as to prevent "gate crashing" or "bombing"
- 3. Manage meeting ID and password**
Design a meeting ID and password specifically for the teaching / meeting; do not re-use the password; send the password separately to participants only
- 4. Don't use public Wi-Fi**
Set encryption for Wi-Fi network

During online teaching / video-conferencing

- 5. No unauthorised admission**
Select the "Lock Meeting" function to bar strangers from joining the meeting
- 6. Be in control**
Only the teacher and the host can share the screen; allow screen sharing on a need basis only
- 7. Video or audio recording only when necessary**
Disable recording; if recording is necessary, notify participants beforehand
- 8. Mind participants' activities**
Monitor content shared by participants; remove inappropriate information and unidentified persons

For Students and Meeting Participants

- 9. Use virtual background**
Use virtual background or background-blurring function to prevent privacy from being captured or disclosed
- 10. Facilitate accurate identification**
Avoid using misleading names or online nicknames so that the teacher or the host can readily identify those attending
- 11. Watch out for suspicious activities**
Keep a close watch of any unusual activities on the account
- 12. What to do in case of data leakage**
Document damage incurred for necessary follow-up action

For App Developers

- 13. Privacy-by-Design**
Adopt the new concept of assessing and addressing possible privacy risks at the design stage of the App



Guidelines published by PCPD on privacy issues arising from COVID-19

Guidelines on privacy issues arising from COVID-19

- PCPD issued guidelines covering:
 - employers' collection of employees' health data and travel history
 - children privacy
 - data security for video conferencing apps
 - Collection of personal data of persons under quarantine
- Disseminated via press releases and various social media platforms





The situation in the mainland of China

Personal data and big data are fundamental ingredients of the mainland Chinese government's pandemic control measures:

1) Real-name registration on public transport



South China Morning Post

SIGN IN/UP

C

Tech firms help Chinese authorities launch real-name registration on public transport for coronavirus tracking

- New systems by tech firms Meituan and Dida require commuters to provide personal information before taking public transport in some Chinese cities
- The initiative is meant to help authorities track those who might have been in contact with individuals infected with the novel coronavirus



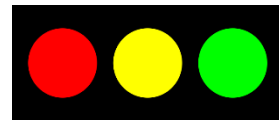
Sarah Dai in Beijing

Published: 5:30pm, 11 Feb, 2020

[Why you can trust SCMP](#)

Source: SCMP (2020)

25



WORLD | ASIA | CHINA

China Turns to Health-Rating Apps to Control Movements During Coronavirus Outbreak

Tech giants such as Alibaba and Tencent tapped to develop color-coded systems to classify people based on their health conditions and travel history



As the number of coronavirus cases rises, epidemiologists around the world look at maps, flight bookings and population data to estimate the size of the outbreak--and explain why their results are higher than China's official tally. Photo: Getty Images

By [Liza Lin](#)

Updated Feb. 18, 2020 8:42 pm ET

2) Health-Rating APPs developed by the mainland Chinese Tech Giants

- Categorise citizens based on their risks of infection (red, yellow or green)
- Those with **red** and **yellow** health codes will face travel restrictions

Source: WSJ (2020) 26

China adapts surveying, mapping, delivery drones to enforce world's biggest quarantine and contain coronavirus outbreak

- Shenzhen Smart Drone UAV's drones used in surveying, mapping can lift a maximum payload of 15kg
- Adaptation shows how outbreak has opened the door for innovative applications to emerge from existing tech



Yujing Liu

Published: 8:00am, 5 Mar, 2020 -

[Why you can trust SCMP](#)

971



3) Drones

➤ Drones modified to fight COVID-19, e.g.-

- disperse public gatherings
- issue warnings to individuals
- remotely check people's temperatures
- spray disinfectants and
- enforce home quarantine orders

Source: SCMP (2020)

27



4) Telecom carriers utilising user data pool

- Chinese telecom companies leverage the data pool of China's billion-plus smartphone users to offer insights
- Help monitor the traffic to help local governments take better precautionary measures



Telecom companies swear by user privacy

By Ma Si | China Daily | Updated: 2020-03-04 08:28



A community worker in Hangzhou, capital of Zhejiang province, checks a resident's health code using a smart phone. The code is part of local efforts to use big data in the fight against novel coronavirus. [Photo by Dong Xuming/For China Daily]

Source: China Daily (2020)

Mainland government's measures to address privacy concerns amidst COVID-19

1) *“Notice on the Protection of Personal Information when Using Big Data for Joint Support and Defense”*

- Released by the Cyberspace Administration of China in February 2020
- **Emphasising privacy principles and cybersecurity requirements** on the collection, use, and disclosure of personal information for purposes of containing COVID-19

Mainland government's measures to address privacy concerns amidst COVID-19 (cont.)

2) Urgent notice issued by the Ministry of Transport

- Issued to public transport operators in January 2020.
- Stipulating that **passenger information collected** in connection with COVID-19 prevention and control shall be **disclosed only to health authorities**.

Mainland government's measures to address privacy concerns amidst COVID-19 (cont.)

3) Notice issued by the National Health Commission

- Issued in February 2020 to all local health commissions.
- Stating the government's policy to strengthen the protection of privacy by **enhancing cybersecurity and ensuring the regulated use of personal data.**

Proposals made by representatives during the “Two Assemblies” of China in May 2020

*Temporary/ad-hoc measures of collecting personal data for fighting COVID-19 should be cancelled after the pandemic, and **not made permanent**.*

Liu Xiaobing, Dean, Public Economy and Management, Shanghai University of Finance

Lian Yu Ming, Head, International Institute for Urban Development, Beijing

*A **regulatory body** should be set up with reference to Hong Kong’s PCPD.*

*Explore the establishment of **guidelines and standards** for the collection of personal data during extraordinary periods.*

Robin Li, CEO, Baidu



What is new norm after COVID-19?

More surveillance and less privacy?

- Continuing the “track and trace” pattern
- Public health and Privacy are on the same side
- Embed data protection principles in the measure that may threaten our privacy
- Be transparent and explainable → **BUILD TRUST**

Contact Us



- ☐ 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, HK

Copyright



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.

