Guest Lecture at the School of Law,
The City University of Hong Kong
28 February 2023 (Tue)

Data Privacy in the Cyberworld

Ms. Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data

Outline

1. Highlights of the Personal Data (Privacy) Ordinance (PDPO)
2. Privacy issues in relation to mobile apps
3. Privacy by design
4. Offences under the PDPO in relation to online activities
   a) Direct marketing
   b) Doxxing

1 Highlights of the Personal Data (Privacy) Ordinance (PDPO)

What is personal data?

Personal data means any data —

(Section 2(1) of the PDPO)

Relating directly or indirectly to a **living individual**;

From which it is practicable for the **identity** of the individual to be directly or indirectly **ascertained**; and

In a form in which **access to or processing of** the data is **practicable**

Who are involved?

Data Subject

The individual who is the **subject** of the data

Data User

A person who, either alone or jointly or in common with other persons, **controls** the **collection**, **holding**, **processing** or **use** of the data

Data Processor

A person who –

a) Processes personal data **on behalf of another person**; and
b) Does **not** process the data for any of the person's **own purposes**

General requirements of personal data protection

(Schedule 1 to the PDPO)

❖ **6 Data Protection Principles (DPPs)**:

- Represent the core requirements of the PDPO
- Cover the entire **lifecycle** of the handling of personal data, from **collection, holding, processing, use** to **deletion**
- Data users have to comply with the DPPs

Six data protection principles (DPPs)

1 收集目的及方式 Collection Purpose & Means

資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應直接與其職能或活動有關。

須以切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移給哪類人士。

收集的資料是有實際需要的，而不超乎適度。

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.

All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred.

Data collected should be necessary but not excessive.

2 準確性、儲存及保留 Accuracy & Retention

資料使用者須採取切實可行的步驟以確保持有的個人資料準確無誤，而資料的保留時間不應超過達致原來目的的實際所需。

Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used.

3 使用 Use

個人資料只限用於收集時述明的目的或直接相關的目的，除非得到資料當事人自願和明確的同意。

Personal data is used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent is obtained from the data subject.

4 保安措施 Security

資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

A data user needs to take practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

5 透明度 Openness

資料使用者須採取切實可行的步驟來公開其處理個人資料的政策和行事方式，並交代其持有的個人資料類別和用途。

A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

6 查閱及更正 Data Access & Correction

資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

A data subject must be given access to his personal data and to make corrections where the data is inaccurate.

DPP1— Purpose and Manner of Collection of Personal Data

- Must be collected for a lawful purpose directly related to a **function** or **activity** of the data user
- The means of collection must be **lawful** and **fair**
- The data is **necessary**, **adequate** but **not excessive** in relation to the purpose of collection
- **All practicable steps shall be taken to inform** the data subject whether it is obligatory to supply the personal data, **the purpose** of data collection, and **the classes of persons to whom the data may be transferred**, etc.

Case sharing – “fair” means of collection (AAB 5/2012; AAB 6/2012)

- 3 celebrities complained that photos of their daily lives and intimate acts at home were taken at a place outside their home, and were published in a magazine without their consent
- AAB: the means of collection was **unfair**:
  - Engaged in personal activities in residential premises
  - The personal activities could not be seen by any passer-by unless vision enhancing devices were used
  - No consent was obtained
- The celebrities had “**reasonable expectation**” of their privacy at the residence

DPP3—Use of Personal Data

❖ Personal data shall not, without the **prescribed consent** of the data subject, be **used for a new purpose**

"*Prescribed consent*" means (i) the express consent of the person given voluntarily; and (ii) has not been withdrawn

"*New purpose*" means any purpose other than the original purpose or its directly related purpose when the data was collected

Consequences of contravention of DPPs

Contravention of a DPP is **not a criminal offence**

NOTE

However, if the data user is found to have contravened the requirements of the PDPO (*including the **DPPs***), the PCPD may **serve an enforcement notice** on the relevant data user (*S.50*)

Non-compliance with an enforcement notice or repeated contravention by the same act is a criminal offence (S.50A)

2 Privacy issues in relation to mobile apps

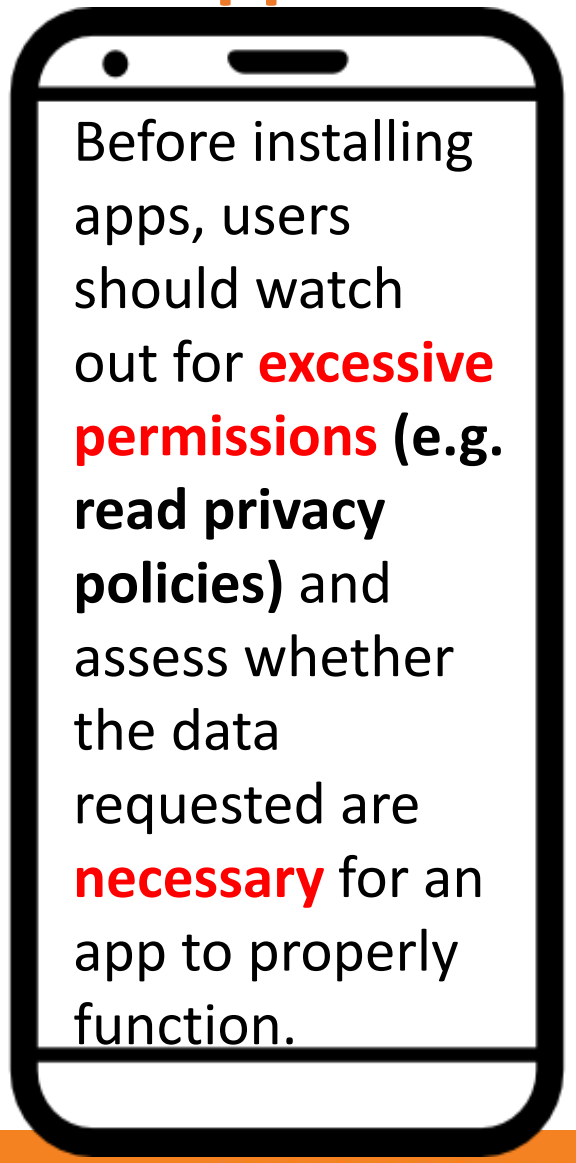
Collection of excessive personal data by mobile apps

- The average person uses **9 mobile apps each day** and **30 apps each month** (Buildfire, 2023)
- Many mobile apps request access to data on our mobile devices
- Some of these data requested can be **privacy-intrusive** (e.g., contacts; geolocation, browsing history, photo liability)

A study by CyberNews on Android apps (2022)

Among the top 1,020 Android apps:

- **36%** requested camera permissions
- **33%** wanted to track users' location
- **21%** requested access to users' microphone



PCPD's study: Comparison of Privacy Settings of Social Media

- Objective: **Inspect the privacy policies of 10 popular social media platforms**, and provide **recommendations on enhancing the protection of personal data privacy**

Findings of PCPD's Study

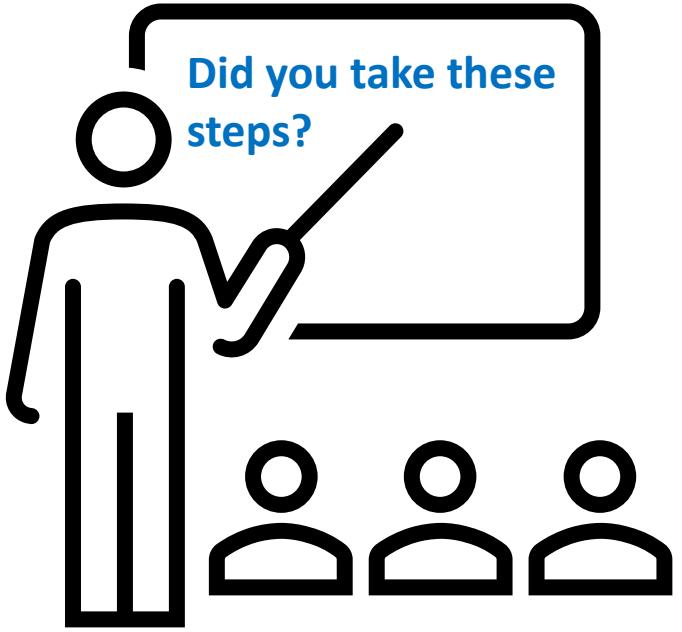
- All the social media reviewed have **privacy policy in place.** They collect a wide variety of personal data, ranging from 12 to 19 types of personal data, **including location data.**
- All the privacy policies explicitly state that users' personal data would be **transferred to their affiliated companies**.
- Twitter, WeChat & YouTube get the highest scores for **readability of privacy policies**.
- Twitter does not provide its privacy policy in **Chinese text**.
- Apart from WeChat, all other instant messaging applications reviewed deploy **end-to-end encryption** in the transmission of messages between users.
- Except for LINE, all other social media reviewed provide **two-factor authentication**.
- Facebook, LINE, WeChat and YouTube all allow users to **disseminate posts to specific individuals or groups**, and **modify the privacy settings** of the contents after posting.

PCPD's study: Comparison of Privacy Settings of Social Media

- PCPD's recommendations to **social media platforms** :
  - Adopt "**Privacy by Design**" to enhance the services
  - **Collect** only the **necessary personal data**
  - Improve the **readability of privacy policies**
  - **Block** the **location tracking** function **by default**
  - Enable **end-to-end encryption** of messages and adopt **two-factor authentication**
  - **Proactively handle all illegal or privacy-intrusive behaviours** (e.g., doxxing, data scraping)

PCPD's study: Comparison of Privacy Settings of Social Media

- PCPD's recommendations to **users of social media**:
  - **Read the privacy policy** before registering an account
  - Create an email address dedicated for social media
  - Only provide the required personal data
  - **Check the default settings** on security or privacy to minimise the disclosure of personal data
  - **Turn off the location tracking** function by default
  - Select the **appropriate settings** before posting contents
  - Use **strong passwords** and enable **two-factor authentication**
  - **Avoid transactions** on social media platforms over public Wi-Fi or unsecured Wi-Fi connections

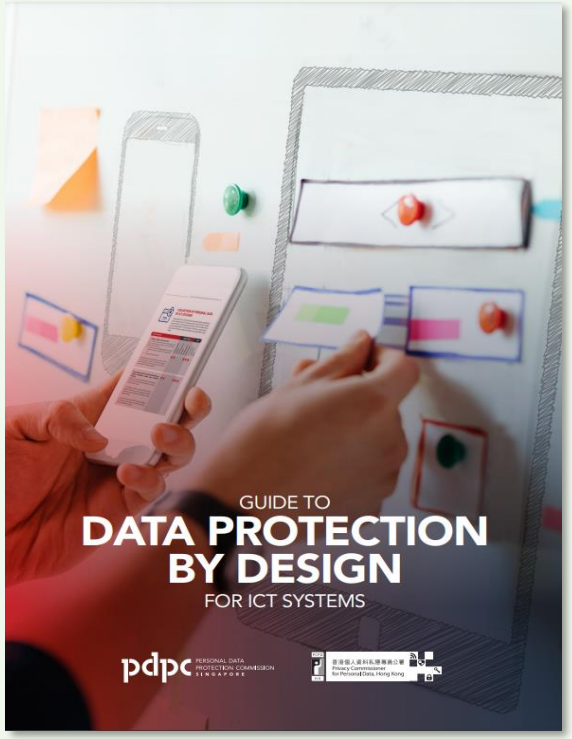


3 Privacy by Design

Privacy by design

What is Privacy by Design?

Proactively and directly **building privacy into the design and operation** of IT systems, networked infrastructure, and business practices



Guide to Data Protection by Design for ICT Systems

- To introduce to organisations **7 DPbD principles**
- To recommend good data protection practices

7 Data-Protection-by-Design Principles

1. Proactive and preventive

Assess, identify, manage, and prevent any data security risks before a data breach occurs

2. Data protection as the default

Integrate data protection measures into the processes and features of the systems, and provide these measures as default settings

3. End-to-end security

Incorporate good data security features and practices at every stage of the Software Development Lifecycle

4. Data minimisation

Collect and store only those personal data that are relevant and necessary for the data processing purpose

5. User-centric

Develop and implement the ICT system with individuals in mind; Provide a user-friendly interface for users to customise privacy settings

6. Transparency

Inform individuals of what personal data are collected from them, how they will be used, and how they will be shared with third parties

7. Risk minimisation

Identify and mitigate all data security risks when designing and using the ICT system

Guidance on the Ethical Development and Use of Artificial Intelligence

7 Ethical Principles for AI

Accountability
Organisations should:
- Be responsible for their actions
- Be able to provide sound justifications for the actions

Human Oversight
The level of human involvement should be proportionate to the risks and impact of using AI

Transparency & Interpretability
Organisations should:
- Disclose their use of AI and the relevant data privacy policies
- Improve the interpretability of automated decisions

Data Privacy
Organisations should:
- Put effective data governance in place to protect personal data privacy

Fairness
Organisations should:
- Treat individuals in a reasonably equal manner, without unjust bias or unlawful discrimination

Beneficial AI
The use of AI should:
- Provide benefits to stakeholders
- Minimise harm to stakeholders

Reliability, Robustness & Security
AI systems should:
- Operate reliably
- Be resilient to errors
- Be protected against attacks

4 Offences in relation to online activities

Direct Marketing

"**Direct marketing**" (DM) means (s.35A(1)):

a. the offering, or advertising of the availability, of goods, facilities or services; or

b. the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes

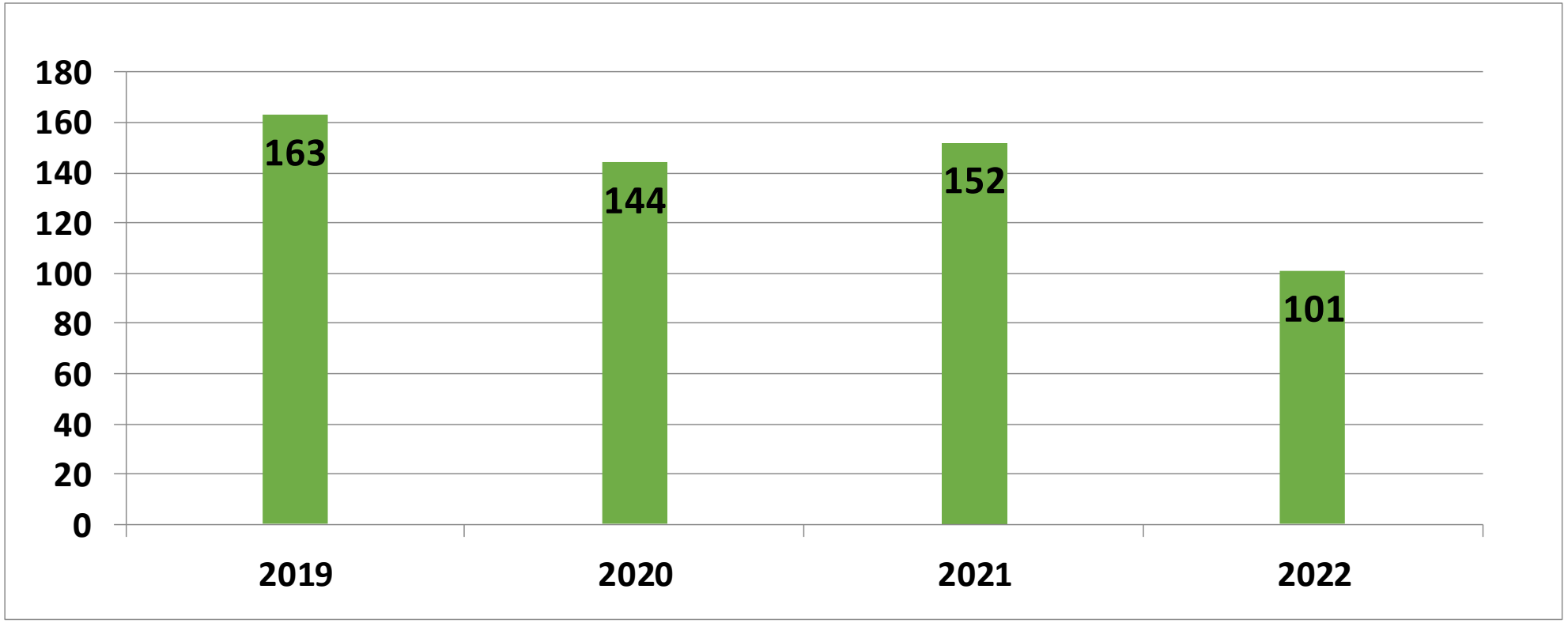
through **direct marketing means**.

a. Sending information or goods, **addressed to specific persons by name**, by mail, fax, electronic mail or other means of communication; or

b. Making telephone calls to **specific persons**

- Direct marketing takes place in many forms (e.g. through mail, telephone calls, emails)
- **E-marketing** means the marketing of goods and services through the Internet (e.g., e-newsletters)
- If an e-marketing activity constitutes "direct marketing", the businesses should comply with the regulatory requirements for direct-marketing

Number of DM related complaints



Requirements for DM under the PDPO

Steps that a data user must take for:

	Using personal data in DM (s.35B – s.35H)	Providing personal data for use in DM (s.35L – s.35M)
Inform the data subject (s.35C(2)(a); s.35J(2)(a))	• The data user intends to so use the personal data; and • He may not do so unless he receives consent	• In writing, that the data user intends to so provide the personal data; and • He may not do so unless he receives written consent
Provide the data subject with information regarding (s.35C(2)(b)&(c); s.35J(2)(b))	• Kinds of personal data to be used; • Classes of marketing subjects; and • A channel for the data subject to communicate his consent	• The personal data is provided for gain (if applicable); • Kinds of personal data to be provided; • Classes of persons to which the data is to be provided; • Classes of marketing subjects; and • A channel for the data subject to communicate his consent
Receive from the data subject (s.35E(1)(a)&(b); s.35K(1)(a))	• Oral consent; or • Written consent	• Written consent

Data subjects have the rights to opt-out without charge

Criminal offences and penalties regarding DM

Offence	Max penalty: Not for gain	Max penalty: For gain
A **data user** who **uses** a data subject's personal data in DM **without** observing **any of the following**: 1. Having received the data subject's consent to the intended use; 2. (If the consent is given orally) Having sent a written confirmation to the data subject within 14 days from receiving the consent, confirming: (a) Date of receipt of the consent; (b) Permitted kind of personal data; and (c) Permitted class of marketing subjects. 3. The use of the personal data is consistent with the data subject's consent.	$500,000 fine 3 years imprisonment	
A **data user** who, when **using** a data subject's personal data in DM for the first time, **fails** to inform the data subject that the data user must, without charge, cease to use the data in DM if the data subject so requires.		
A **data user** who **fails** to comply with the data subject's requirement to **cease to use** personal data in DM without charge.		
A **data user** who **provides** the data subject's personal data to another person for use in DM **without** observing **any of the following**: 1. Having received the data subject's written consent to the intended provision of personal data; 2. (If the data is provided for gain) Having specified in the information provided to the data subject the intention to so provide; 3. The provision of the data is consistent with the data subject's consent.	$500,000 fine 3 years imprisonment	$1,000,000 fine 5 years imprisonment
A **data user** who **fails** to comply with a data subject's request to: **1.** **Cease to provide** the data subject's personal data for use in DM; or 2. Notify any data transferee in writing to cease to use the data in DM.	$500,000 fine 3 years imprisonment (in any other case)	
A **data transferee** who **fails** to comply with a data user's written notification to **cease to use** a data subject's personal data in DM.	$500,000 fine 3 years imprisonment	

Case sharing: Chinese medicine practitioner convicted of DM offences

Case facts

- The **Complainant (patient of a Chinese medicine clinic) provided her personal data to the clinic** in 2015.
- The Defendant worked at the clinic at the time. The Complainant had **never consulted the Defendant**.
- In 2020, the Complainant **got a WhatsApp message from the Defendant**, **promoting** the **service** of her new clinic.
- The complainant **considered that the Defendant used her personal data for DM without her consent**. She lodged a complaint with the PCPD.
- The PCPD referred the case to the Police for criminal investigation.

Court's ruling

- In October 2022, the Defendant was charged under sections 35C(1) and 35F(1) of the PDPO for **failing to take the necessary actions and obtain the data subject's consent** before using her personal data in direct marketing.
- On 10 Feb 2023, the **Defendant pleaded guilty**.
- She was **fined $4,000**.

Amendments to the PDPO to curb illegal doxxing acts

I

Create 2-tiers of offences to **curb doxxing acts**

II

Empower the Commissioner to carry out **criminal investigation and institute prosecution**

III

Confer on the Commissioner power to issue **cessation notices**

(I) Section 64 – Create offences to curb doxxing acts

	Summary offence (1st tier)	Indictable offence (2nd tier)
1.	Any personal data of a data subject is disclosed without the relevant consent of the **data subject**	
2.	Has an **intent** or is being **reckless** as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject	
3.	N/A	The **disclosure causes any specified harm** to the data subject or any family member of the data subject
4.	Maximum penalties: A fine at level 6 (**$100,000**) and to imprisonment for **2 years**	Maximum penalties: A fine of **$1,000,000** and to imprisonment for **5 years**

(II) Empower the Commissioner to carry out criminal investigation and institute prosecution

Issue written notice to request any person to provide relevant material; or to answer relevant question to facilitate investigation
(new section 66D of the PDPO)

The Commissioner may

Apply for warrant to enter and search premises and seize materials for investigation; or access electronic device (and decrypt any material stored therein)
(new section 66G of the PDPO)

To stop, search and arrest, without warrant, any person who is reasonably suspected of having committed a doxxing-related offence
(new section 66H of the PDPO)

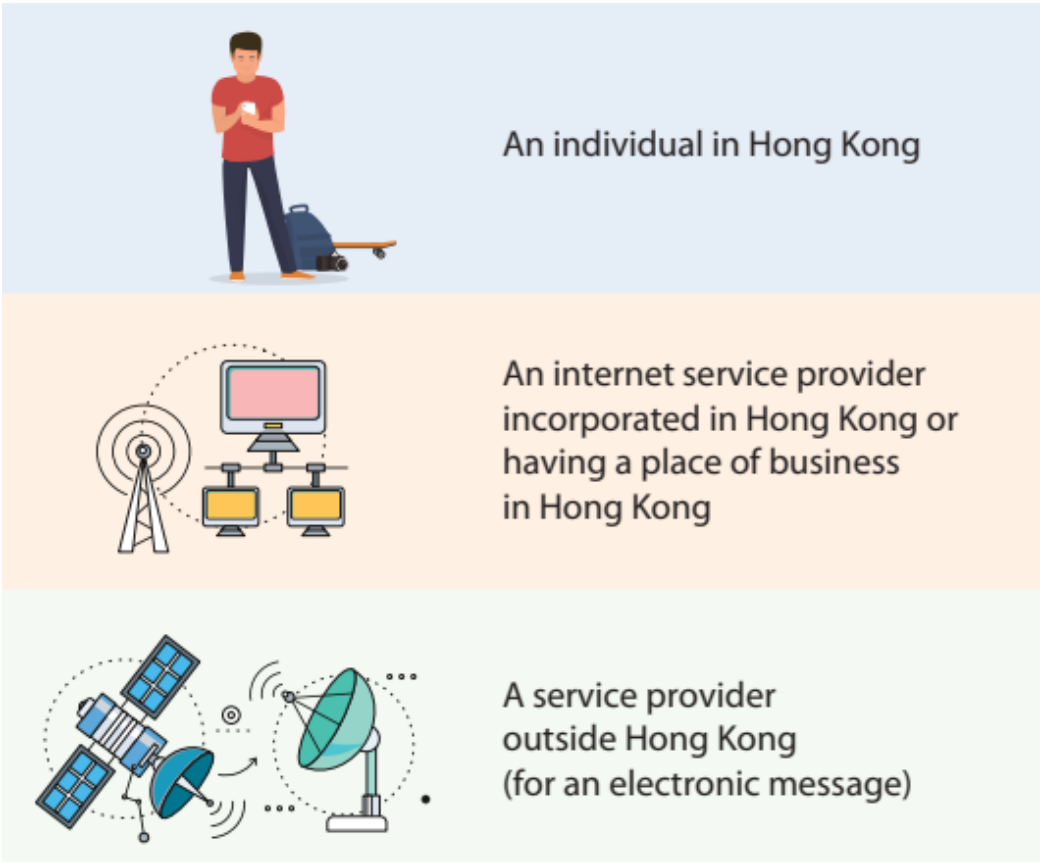
Prosecute in the name of the Commissioner a doxxing-related offence triable summarily in the Magistrates' Court
(new section 64C of the PDPO)

(III) Confer on the Commissioner power to issue cessation notices

- **The Commissioner can serve a cessation notice where there is a disclosure, with the requisite intent or recklessness, of personal data without the data subject's consent.**

- **The cessation notice will be sent to a person who is able to take a cessation action to remove the doxxing message, including:**

(New sections 66K, 66L and 66M of the PDPO)



Thank you!

- Hotline : 2827 2827
- Fax : 2877 7026
- Website : www.pcpd.org.hk
- E-mail : communications@pcpd.org.hk
- Address: Room 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong