

# Data Protection Insights from Regulators in Hong Kong & Macau

1 November 2019 | Huawei Headquarters, Shenzhen

## Data Protection in Hong Kong from a Regulatory Perspective

Stephen Kai-yi WONG, Barrister

Privacy Commissioner for Personal Data, Hong Kong, China

1



• Home / Business

## Huawei forges ahead with global commercialization of 5G network

By Yuan Shenggao | China Daily Global | Updated: 2019-10-15 07:38

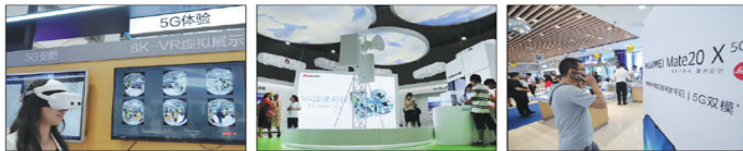


Chinese tech giant Huawei Technologies is pushing ahead with the commercialization of 5G technology, with over 50 contracts signed and 200,000 5G base stations shipped worldwide, a company executive said.

5G, fifth-generation wireless technology, allows users to surf the internet and download data at superfast speeds.

"1G and 2G technology shortened the distance between people by voice and short message. 3G and 4G enriched interpersonal interaction through mobile internet and video. And 5G will bring us to an intelligent world where everything is interconnected," said Peng Honghua, chief marketing officer of wireless business of Huawei, at the Huawei Asia-Pacific Innovation Day held in Chengdu, Sichuan province, in September.

"5G provides the ultimate experience for customers, driving mobile broadband to a new high ground of prosperity. Furthermore, it will promote digitalization and improve efficiency in more industries," he added.



Source: [http://www.chinadaily.com.cn/global/2019-10/15/content\\_37515552.htm#targetText=Chinese%20tech%20giant%20H%20uawei%20Technologies,download%20data%20at%20superfast%20speeds](http://www.chinadaily.com.cn/global/2019-10/15/content_37515552.htm#targetText=Chinese%20tech%20giant%20H%20uawei%20Technologies,download%20data%20at%20superfast%20speeds)

2

# 5G in Hong Kong

- Government allocated spectrum for 5G services to 4 mobile network operators in mid-Oct 2019
- 5G services is expected to roll out in **Q2 of 2020**

Source: <https://www.fiercewireless.com/5g/hong-kong-carriers-scoop-up-3-5-ghz-spectrum-at-5g-auction>

### Hong Kong carriers scoop up 3.5 GHz spectrum at 5G auction

by Bevin Fletcher | Oct 16, 2019 4:04pm



Hong Kong's four mobile operators collectively spent \$128 million for 200 MHz of 5G spectrum in the 3.5 GHz band. (Getty Images)



Quicker connectivity

Higher Bandwidth

Lower Latency

More IoTs, everywhere



More Personal Data  
collected

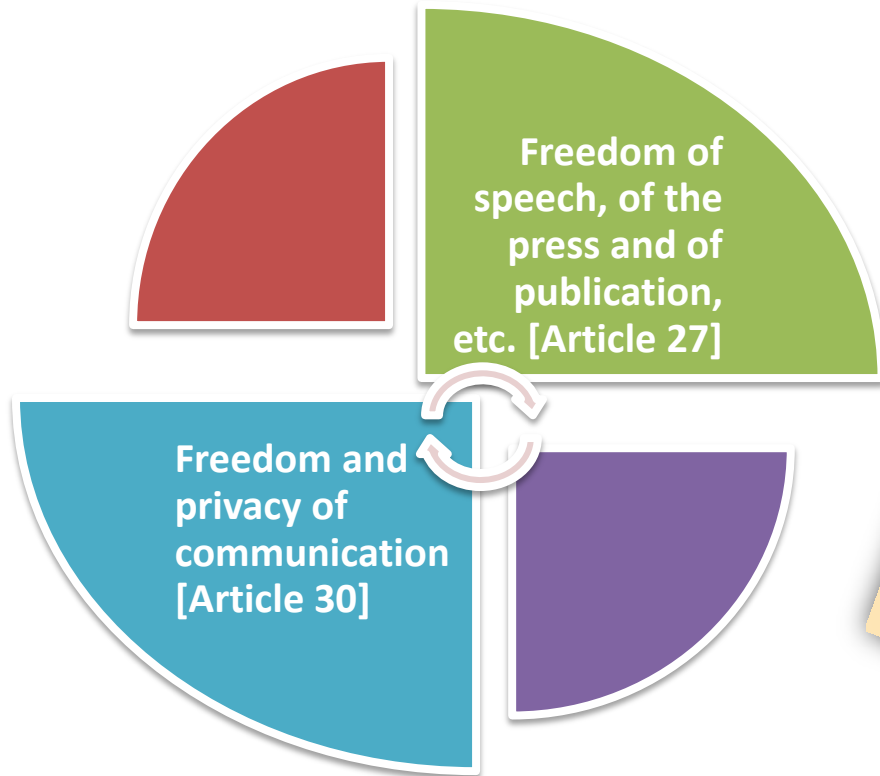
More privacy  
protection warranted

# 1

## Introduction to Hong Kong's Personal Data (Privacy) Ordinance



# The Basic Law (1990)



# Hong Kong Bill of Rights Ordinance (1991)

Protection of privacy, family, home,  
correspondence, honour and reputation

[Art. 14]

*(c.f. ICCPR Art. 17)*



International Covenant on  
Civil and Political Rights

Freedom of opinion and expression

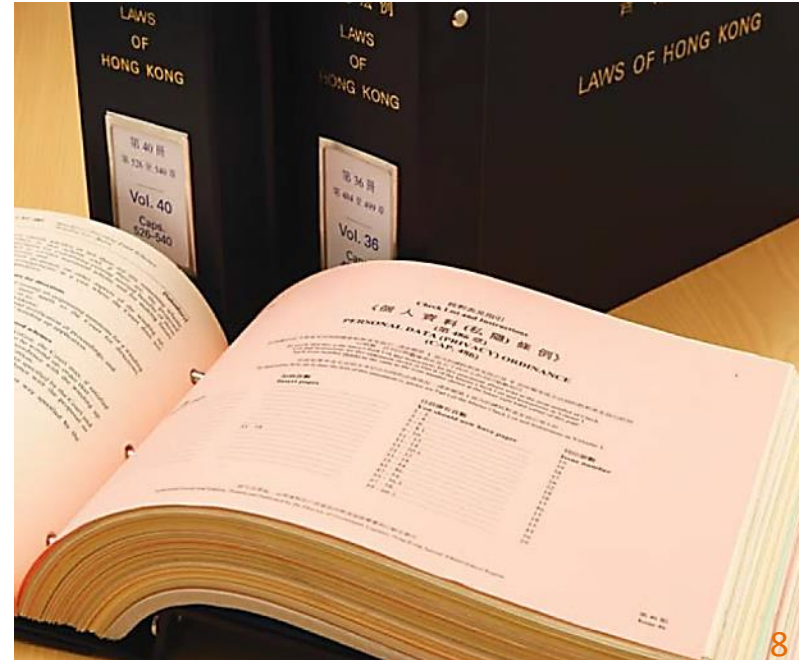
[Art. 16]

*(c.f. ICCPR Art. 19)*

# Personal Data (Privacy) Ordinance

## Cap 486, Laws of Hong Kong

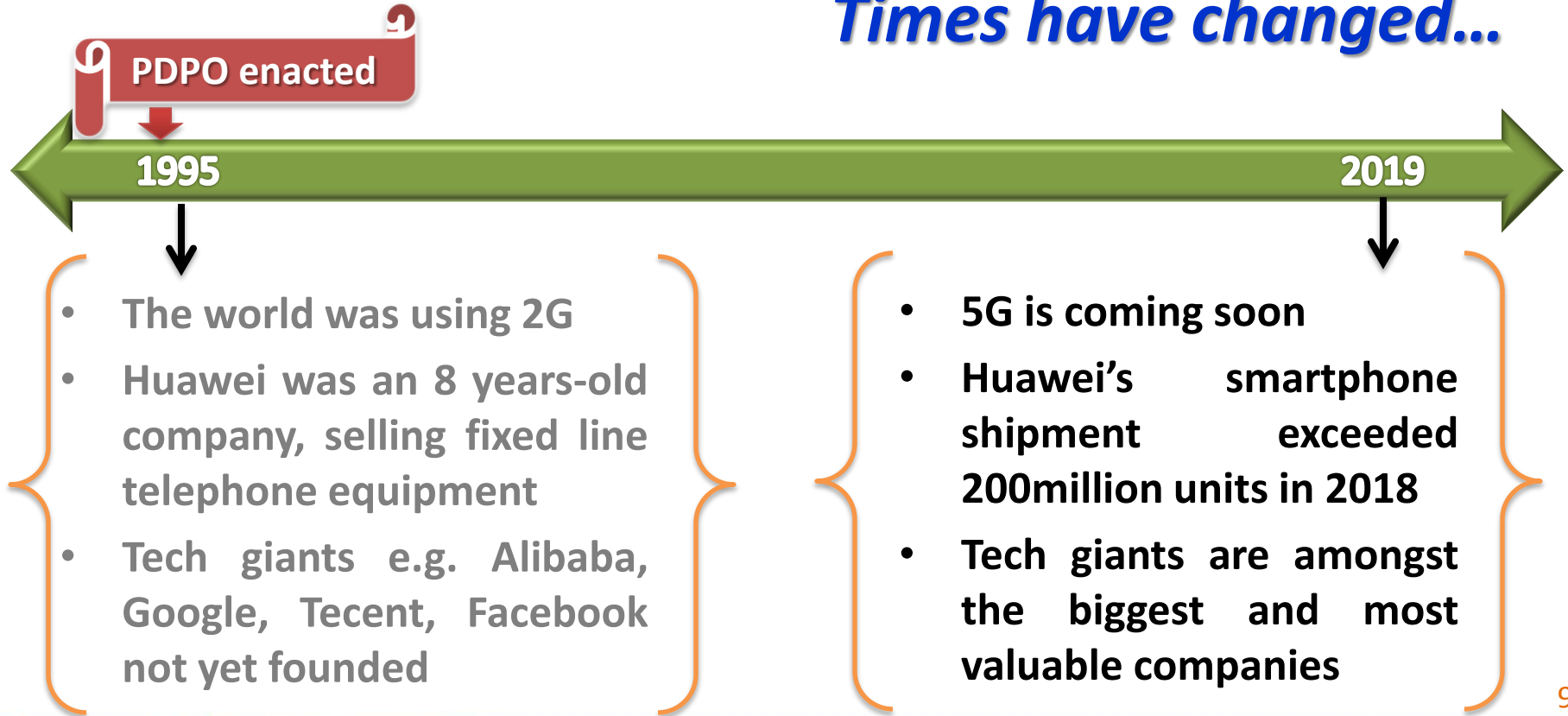
- Enacted in **1995**
- Protects individuals' privacy in relation to **personal data**
- Created **independent** Privacy Commissioner for Personal Data
- Covers the **public** (including the government) and **private sectors**
- Referenced to **1980 OECD Privacy Guidelines** and **1995 EU Data Protection Directive**



8



# Times have changed...



# Personal Data (Privacy) Ordinance (1995)

## Legislative background

### Business Perspective

- To facilitate business environment, maintain Hong Kong as a financial and trading hub

### Human Rights Perspective

- Protect individuals' personal data privacy

# The OECD Guidelines 1980

Organisation for Economic Co-operation and Development

1st generation  
of data  
protection law

Commonly  
used  
internationally

Eight  
fundamental  
data  
protection  
principles



# 1995 EU Data Protection Directive

2nd generation of  
data protection law

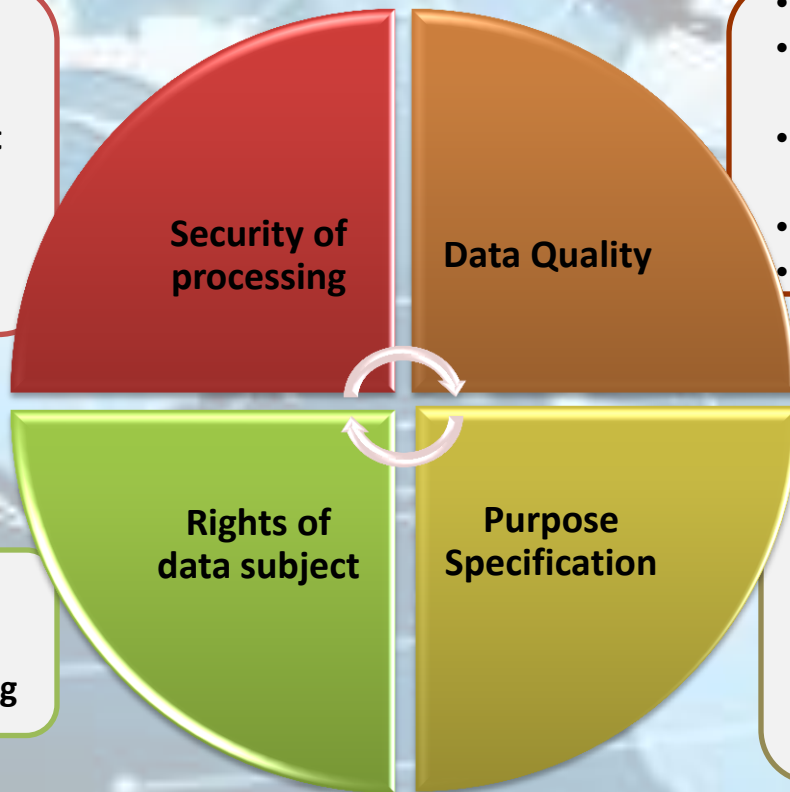
*Set out the model  
legal framework for  
all EU  
national laws*

Replaced by GDPR  
in 2018  
(3<sup>rd</sup> generation of  
data protection law)



# 1995 EU Data Protection Directive

- Implement appropriate technical and organizational measures
- Sufficient guarantees in respect of data security provided by data processor
- Data processor must be governed by a contract



- Fairly and lawfully processed
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than necessary

- Right of access
- Right to rectify
- Right to object processing

- Identity of the controller
- Purposes of the processing
- Recipients or categories of recipients of the data
- Obligatory or voluntary provision of data

# HK: Personal Data (Privacy) Ordinance (1995)



# PDPO vs OECD Guidelines vs 1995 EU Directive

	PDPO	OECD Guidelines	1995 EU Directive
Collection Limitation	√	√	√
Data Quality (necessary for the purposes and accurate)	√	√	√
Use Limitation	√	√	√
Purpose Specification	√	√	√
Openness	√	√	√
Security	√	√	√
Individual Participation	√	√	√
Accountability	X	√	X

# Definition of “Personal Data” under PDPO

“Personal data” (個人資料) means any data -

- (a) relating directly or indirectly to a living individual;
- (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
- (c) in a form in which access to or processing of the data is practicable.

“Data” (資料) means any representation of information (including an expression of opinion) *in any document*.

# Six Data Protection Principles (DPPs) of the PDPO

## 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之實際所需。

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透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 practical 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.



# The “Octopus Incident” 2010

- Found to have profited from sales of membership data to insurance companies for direct marketing without consent
- CEO stepped down
- PDPO amended



Octopus sold personal data of customers for HK\$44m

Phyllis Tsang and Ng Kai

## THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life

ASIA TECHNOLOGY

### Octopus CEO Resigns Over Data Sale

By JEFFREY  
Updated Au

# CHINADAILY

Thursday, Mar 10, 2016

中國日報

Home China Business Metro Beijing Regional World Opinion Spor

Hong Kong

### Octopus chairman to step down in Dec

By Michelle Fei (HK Edition)  
Updated: 2010-10-20 06:57

19

# Amendments in 2012 – Strengthened Regulation on Direct Marketing

- **Provide prescribed information** to individuals (e.g. kinds of personal data to be used, classes of marketing subjects)
- Obtain individuals **consent**
- Allow individuals to **opt out**
- Maximum penalties for contravention: **fine of HK\$5 million + imprisonment for 5 years**

# EXEMPTIONS

Under PDPO (non-exhaustive)

S.52  
Domestic  
purpose

S.58  
Crimes, etc.

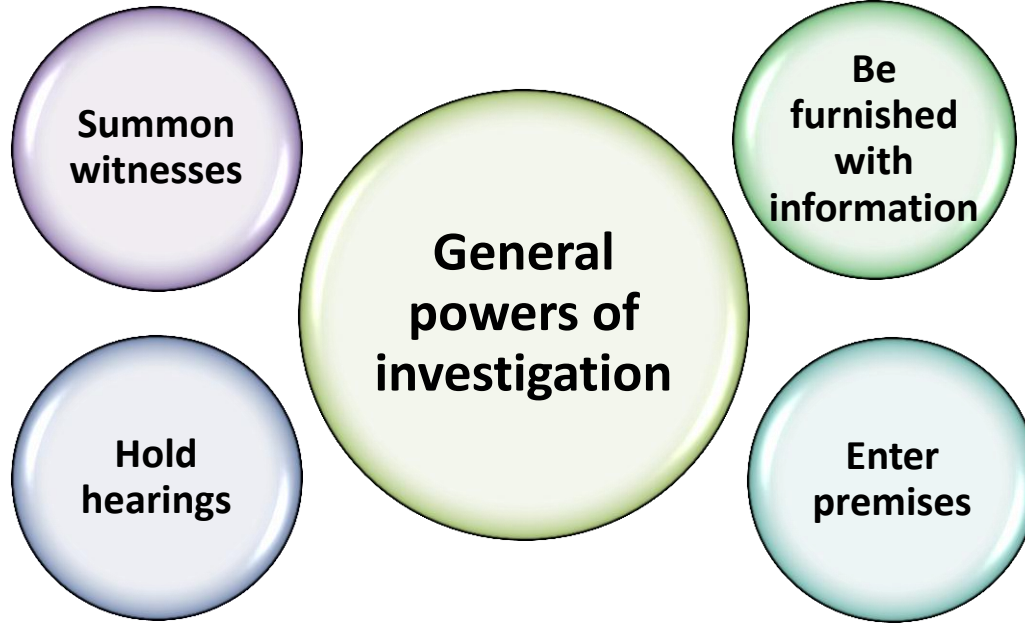
S.60B  
Legal  
proceedings

S.61  
News

S.62  
Statistics and  
research

21

# Enforcement Powers of PCPD



**Obstruction to the exercise of the Privacy Commissioner's investigation power is a criminal offence.**

# Enforcement Powers of PCPD



## Enforcement Actions

- Serve **enforcement notice** on the relevant data user directing the data user to remedy, and if appropriate, prevent any recurrence of the contravention
- Non-compliance with an enforcement notice is a **criminal offence** (maximum fine HK\$50,000 and imprisonment for 2 years, and a daily fine of HK\$1,000 in case of a continuing offence)



# Enforcement Powers of PCPD



## Criminal Investigation and Prosecution

- The Privacy Commissioner **does not have** criminal investigation power
- Referral to the Police for criminal investigation and prosecution by the Department of Justice where appropriate

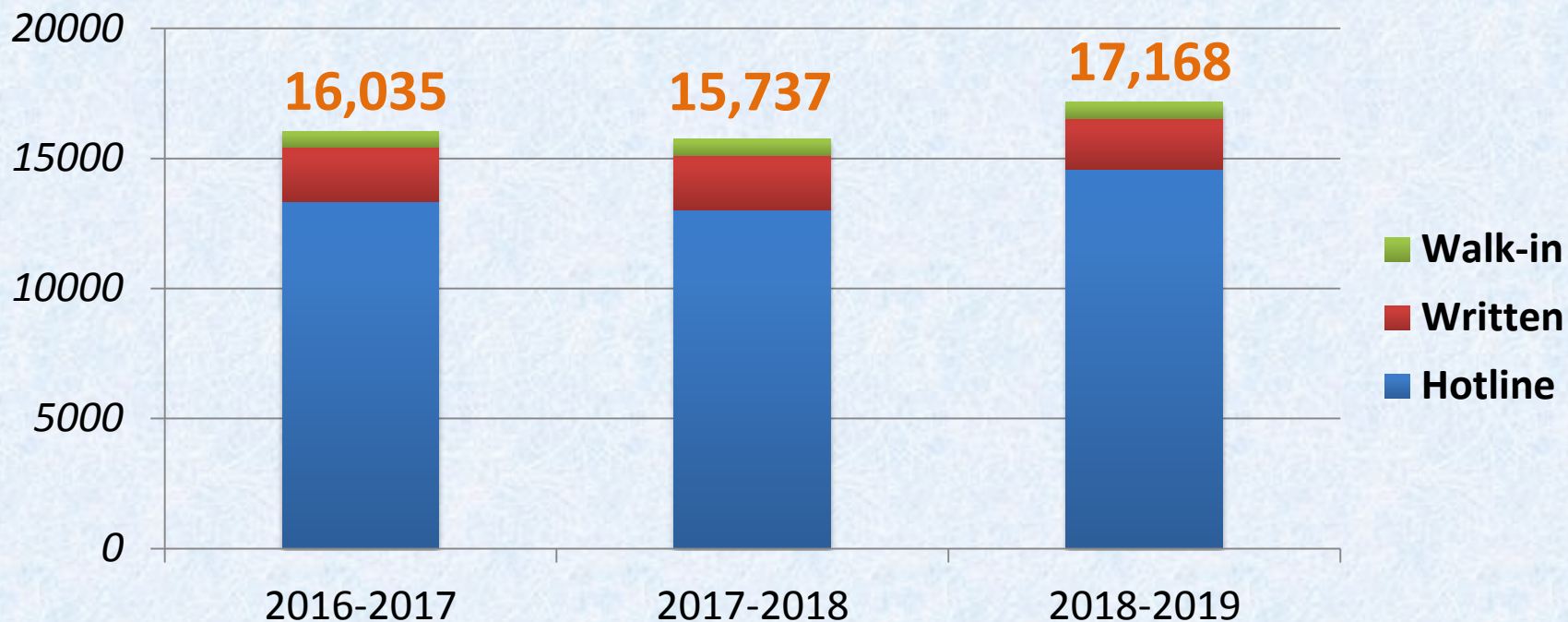
# Enforcement Powers of PCPD

## Civil Claims for Compensation

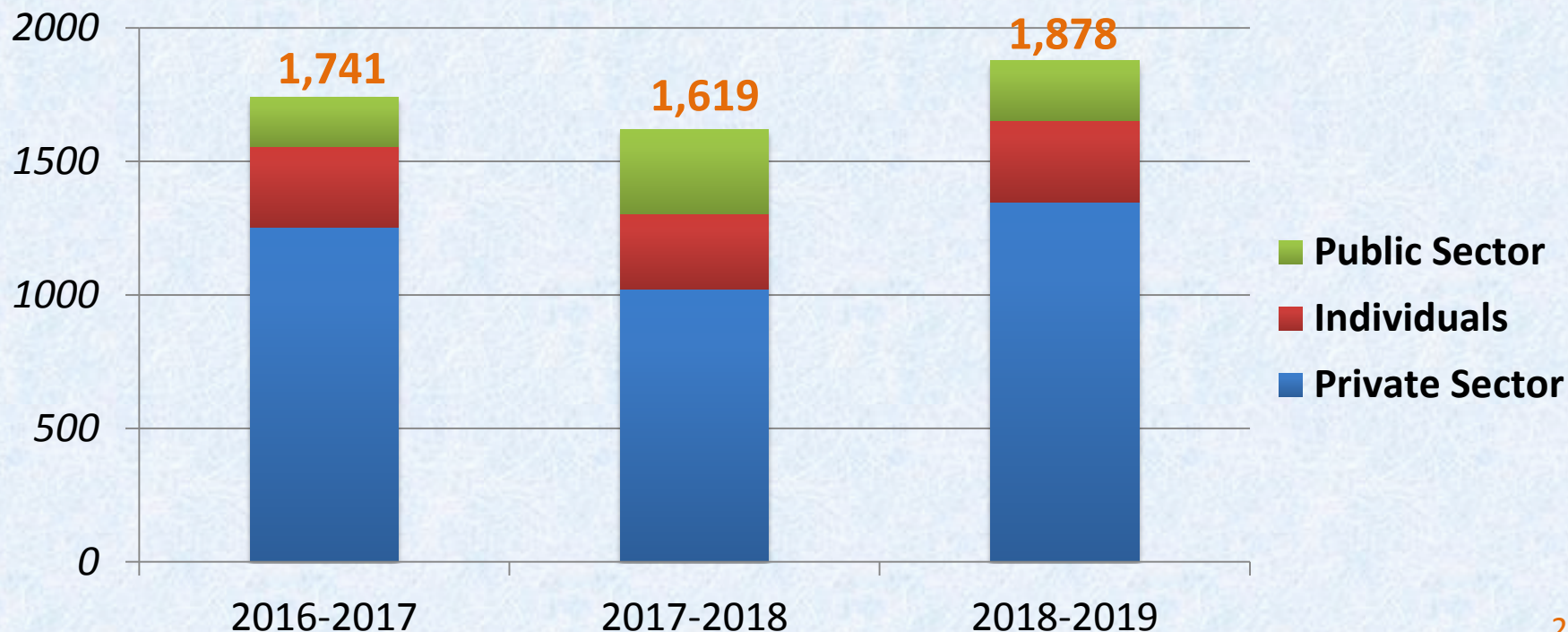


- An individual who suffers damage, including injury to feeling, by reason of a contravention of the PDPO in relation to his personal data, is entitled to obtain compensation from the data user concerned
- The Privacy Commissioner may grant legal assistance to the aggrieved individual

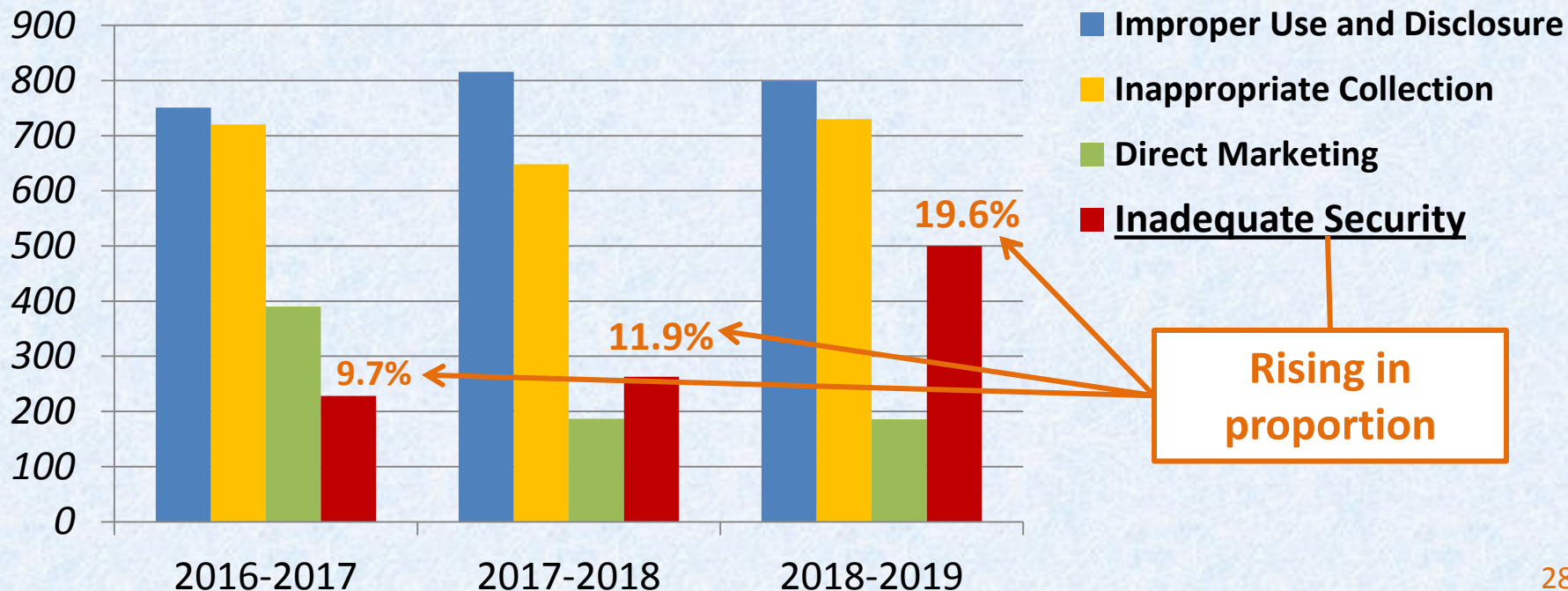
# No. of Enquiries (Recent 3 Fiscal Years)



# No. of Complaints (Recent 3 Fiscal Years)



# Major nature of violations of the PDPO alleged in complaints



# Data breaches reported to PCPD



Year	Affected Data Subjects
2018	9.8M+
2017	3.9M
2016	104K
2015	871K
2014	47K
2013	90K



# In 2018, data of 1.4 billion people around the world were compromised



*...Data breach is a “new norm”*

30

# Data security – *The pressing issues*

IT is  
increasing  
integrated  
into business  
operations

Increase in  
sophistication  
of hackers  
(Hacking as a  
Service, or  
HaaS,  
emerges)

Cyberattack is  
not “if” but  
“when”

# Case study:

## *Data breach of an airline based in HK affecting 9.4m passengers*

### Background

- Data breach notification lodged to PCPD on 24 Oct 2018
- Unauthorised access to airlines information systems
- 9.4 million passengers from over 260 countries / jurisdictions / locations affected
- Personal data involved consisted mainly of name, flight number and date, email address, membership number, address, phone number

# Case study:

## *Data breach of an airline based in HK affecting 9.4m passengers*

### PCPD's investigation and findings

Investigation  
focuses

Data security

Data retention  
period

Contraventions

Various data security failures (see next slides)

Not taking all reasonably practicable steps to erase unnecessary HK Identity Card No. of passengers

# Case study:

## *Data breach of an airline based in HK affecting 9.4m passengers*

### Date security failures include:

- Risk alertness being low 
- Vulnerability scanning exercise at a yearly interval (too lax) 
- Failure to identify and address the commonly known exploitable vulnerability 
- Failure to have an effective personal data inventory 
- Failure to apply effective multi-factor authentication to all remote access users



# Case study:

## *Data breach of an airline based in HK affecting 9.4m passengers*

### PCPD's enforcement action

### **Enforcement Notice**

Engage independent data security expert to overhaul systems

Implement effective multi-factor authentication for remote access

Conduct effective vulnerability scans

Engage independent data security expert to review / tests system security

Devise clear data retention policy, specify retention period(s) and ensure effective execution

Completely obliterate all unnecessary HKID Card numbers

# 2

## Challenges in the digital age



# (1) Excessive collection of personal data

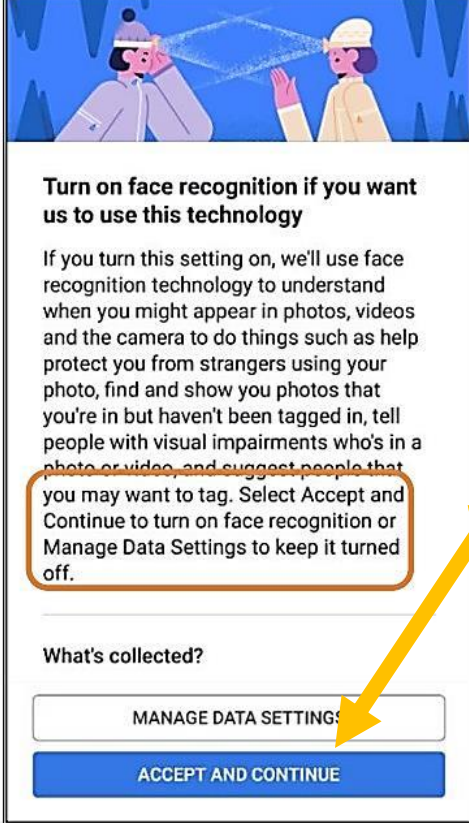
67.2% respondents think smartphone APPs collect unnecessary personal information



## 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:

- 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

Source: Norwegian Consumer Council – “Deceived by Design” (June 2018)

PALO ALTO, Calif. (Reuters) - Uber Technologies Inc is pulling a heavily criticized feature from its app that allowed it to track riders for up to five minutes after a trip, its security chief told Reuters, as the ride-services company tries to fix its poor reputation for customer privacy.

BUSINESS NEWS AUGUST 29, 2017 / 1:02 PM / 2 YEARS AGO

## Uber to end post-trip tracking of riders as part of privacy push

Dustin Volz

4 MIN READ



❖ In 2016, after an update of its app, Uber started asking for permission to **track customers' location even after their rides.**

❖ After facing backlash, Uber **restored users' ability** to share location data only while using the app in 2017.



FILE PHOTO - An Uber sign is seen in a car in New York, U.S. June 30, 2015. REUTERS/Eduardo Munoz/File Photo

The change, which restores users' ability to share location data only while using the app, is expected to be announced on Tuesday and rolled out to Apple Inc iPhone users starting this week. It comes as Uber tries to recover from a series of crises culminating in the ouster of Chief Executive Travis Kalanick and other top executives.

Source: <https://www.reuters.com/article/us-uber-privacy-idUSKCN1B90EN> (29 Aug 2017)

39

## (2) Covert collection of personal data



Westfield's Smart Screen captures your movements as you shop. Source: Supplied



News Corp Australia

National | World | Lifestyle | Travel | Entertainment | Technology | Finance | Sport

finance business > retail

### Westfield is using facial detection software to watch how you shop

- ❑ Hidden facial detection cameras installed inside of advertising light boxes, in large malls in Australia and Newland, for mall runners to analyse the customers and deliver personalised advertisement.
- ❑ They run **without obtaining consent** from customers prior.

Source: <https://www.news.com.au/finance/business/retail/westfield-is-using-facial-detection-software-to-watch-how-you-shop/news-story/7d0653eb21fe1b07be51d508bfe46262> (19 Oct 2017)

40

## Privacy fears after woman says Alexa recorded a private conversation and sent it to a random contact

- Portland woman discovered her Alexa recorded and sent a private conversation
- It was only until a contact let her know that she became aware of the flaw
- Amazon says it's aware of the issue and in the process of releasing a fix
- Issue raised the ire of privacy advocates who worry Alexa is spying on its users

By ANNIE PALMER FOR DAILYMAIL.COM

PUBLISHED: 23:22 BST, 24 May 2018 | UPDATED: 11:52 BST, 25 May 2018



A Portland woman was shocked to discover that Echo recorded and sent audio of a private conversation to one of her contacts without their knowledge.

Source: Daily Mail (24 Mar 2018)

- A user of the Amazon smart home speaker found out that the voice assistant 'Alexa' recorded and sent out a private conversation to her contacts.
- The speaker woke up due to a word in background conversation sounding like the wake word "Alexa". Then the subsequent conversation was heard as a command "send message".

41



### (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

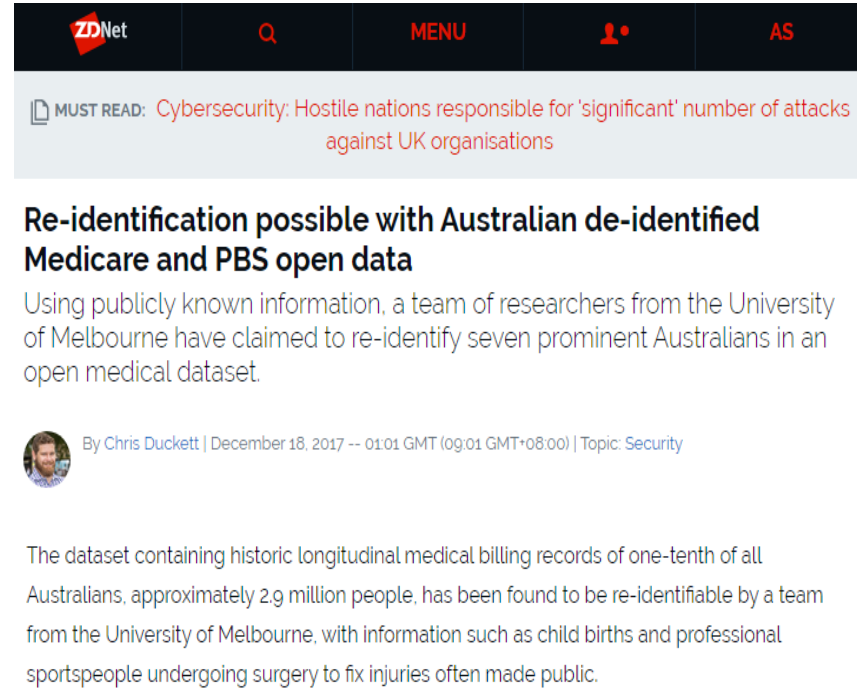
Amplifying privacy and security risks

Data processors not directly regulated by the PDPO

Problematic for:  
Data retention  
Data security

# (4) Profiling and Re-identification

- A team of academics at the University of Melbourne were able to **re-identify a publically available anonymised dataset** consisting medical billing records
- By **linking unencrypted parts** of the record with **publicly known information**, the team re-identified 7 prominent people
- The dataset contained records of **2.9 million people**



The screenshot shows a ZDNet article. At the top, there is a navigation bar with the ZDNet logo, a search icon, a 'MENU' button, a user profile icon, and the text 'AS'. Below the navigation bar is a 'MUST READ' section with a document icon and the text: 'Cybersecurity: Hostile nations responsible for 'significant' number of attacks against UK organisations'. The main article title is 'Re-identification possible with Australian de-identified Medicare and PBS open data'. The sub-headline reads: 'Using publicly known information, a team of researchers from the University of Melbourne have claimed to re-identify seven prominent Australians in an open medical dataset.' Below the sub-headline is a small circular profile picture of Chris Duckett, followed by the text: 'By Chris Duckett | December 18, 2017 -- 01:01 GMT (09:01 GMT+08:00) | Topic: Security'. The main body of the article begins with: 'The dataset containing historic longitudinal medical billing records of one-tenth of all Australians, approximately 2.9 million people, has been found to be re-identifiable by a team from the University of Melbourne, with information such as child births and professional sportspeople undergoing surgery to fix injuries often made public.'

Source: <https://www.zdnet.com/article/re-identification-possible-with-australian-de-identified-medicare-and-pbs-open-data/>



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

South China Morning Post SIGN IN/UP

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 SIGN IN/UP

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)

# Privacy risks of 5G

**Vision of 5G: always available, anytime, anywhere**

**Ubiquitous connection = continuous tracking and monitoring of individuals via smartphones, IoTs, and use of services**

**More IoTs connected to 5G networks, but IoT devices generally have lower security standards, making the risk of data breach higher**

**5G signal ranges are shorter, meaning more cell site may have to be built, which makes the tracking of individual's location more precise than before**

# 3

## Possible reforms of the PDPO in light of digital challenges

# Possible amendments to PDPO in response to ICT developments:

## (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)
<b>Criteria:</b> <ul style="list-style-type: none"><li>• Practicable to <u>ascertain identity</u></li></ul>	<b>Criteria:</b> <ul style="list-style-type: none"><li>• Relating to or about an <u>identifiable</u> individual</li></ul>
<b>Meaning:</b> <ul style="list-style-type: none"><li>• <u>Knowing</u> who a person is</li></ul>	<b>Meaning:</b> <ul style="list-style-type: none"><li>• Able to <u>single out</u> a person, not necessarily knowing who the person is</li></ul>
<b>Result:</b> <ul style="list-style-type: none"><li>• <u>Narrower</u> scope of personal data and <u>less</u> protection to privacy</li></ul>	<b>Result:</b> <ul style="list-style-type: none"><li>• <u>Wider</u> scope of personal data and <u>stronger</u> protection to privacy</li></ul>

# 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



# 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

# 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**

# Recent 'Doxxing' in Hong Kong

- Privacy intrusive/intimidating messages and posts spreading at an alarming rate
- From 14 June to 21 October 2019, the PCPD
  - Received and found **2,683** cases
  - Written **84** times to **13** platforms to request deletion, **612** links (**37%**) removed
  - **1,297** cases have been referred to the Police for investigation



Intimidating message online:  
***“Get prepared to pick up with a linen bag after school”***

# 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
- ❖ Amending the scope of protection to include platforms and webpages that have **relatively close connection to Hong Kong**
- ❖ Give the PCPD powers to **directly issue prohibitive orders** to relevant social media platforms and website (e.g. take down doxxing posts, provide personal data of those posting doxxing messages)

# 4

## The roles of the PCPD

# PCPD's Roles – Enforcer + Educator + Facilitator

## PCPD's Strategic Focus





# Data Ethics and Trust



# Data Ethics

2017

## Ethics on AI -

First being discussed at the ICDPPC meeting held in Hong Kong

2018

*“Ethical Accountability Framework for Hong Kong, China”* published by PCPD

*“Declaration on Ethics and Data Protection in Artificial Intelligence”* made by the ICDPPC in Brussels

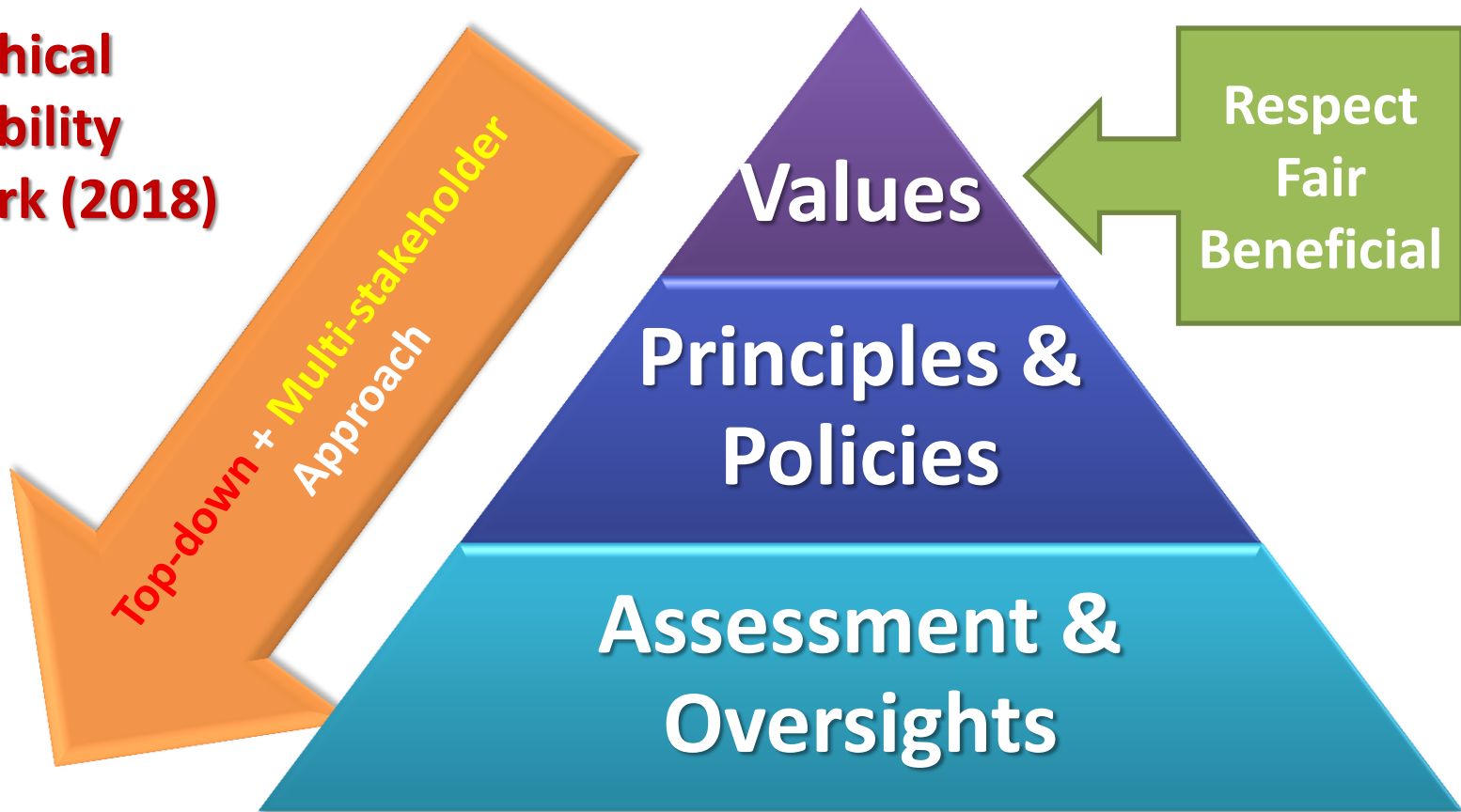
**ICDPPC Permanent Working Group on Ethics and Data Protection in AI** established (co-chaired by CNIL, EDPS and PCPD/HK)

2019

*“Ethics Guidelines for Trustworthy AI”* issued by the European Commission

59

# PCPD's Ethical Accountability Framework (2018)



# HKMA'S CIRCULAR ON 3 MAY 2019

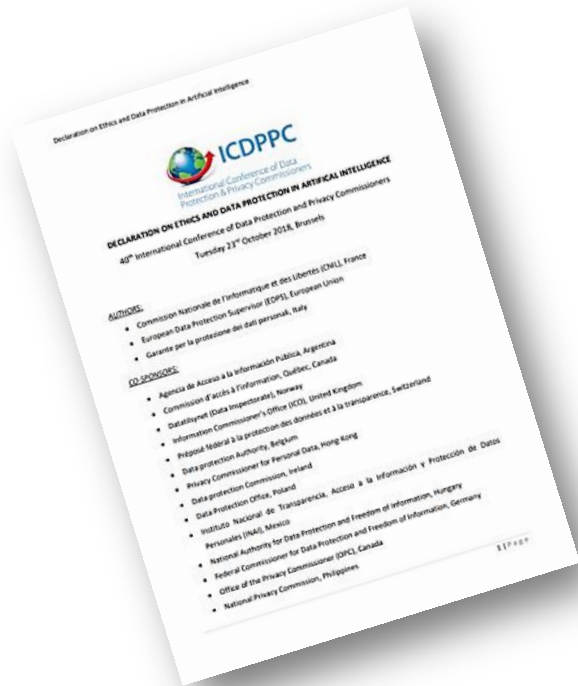


- To all authorized institutions
- Expressing support to PCPD's concept of data ethics and stewardship
- Encouraging adoption of PCPD's Ethical Accountability Framework in development of Fintech in order to-
  - Address privacy concerns of customers
  - Enhance customers' trust in using Fintech

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

61

# ICDPPC Declaration on Ethics and Data Protection in Artificial Intelligence (October 2018): Six Core Principles



Reducing  
biases or  
discriminations

Empowerment  
of every  
individual



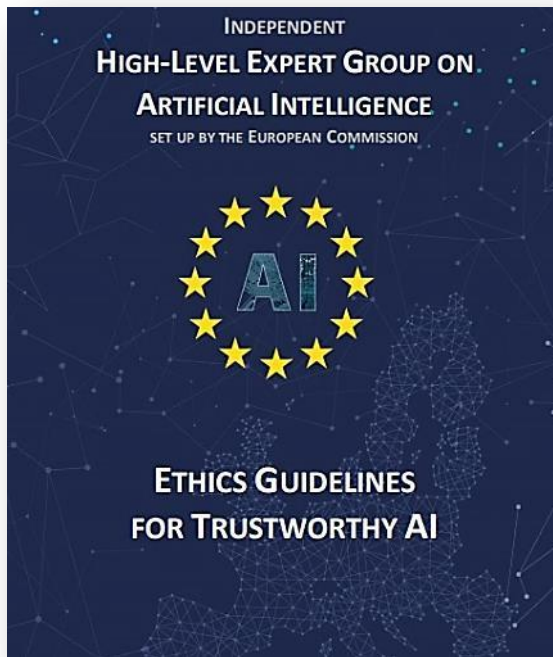
Fairness  
principle

Continued  
attention  
and vigilance

Systems  
transparency  
and  
intelligibility

Ethics by design

# EU's "Ethics Guidelines for Trustworthy AI" (2019)



## 7 key requirements:

1. Human agency and oversight
2. Technical robustness and safety
3. Privacy and data governance
4. Transparency
5. Diversity, non-discrimination and fairness
6. Societal and environmental well-being
7. Accountability

# ISO/IEC 27701:2019

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

- World's first international standard for managing privacy information
- Building on ISO 27001 and ISO 27002
- Assisting in compliance with personal data protection laws
- Four core parts:
  - ❖ Personal information management system
  - ❖ Information security techniques and good practices
  - ❖ Guidance for PII controllers (i.e. data users)
  - ❖ Guidance for PII processors (i.e. data processors)



***“NIST Privacy Framework: A Tool  
for Improving Privacy Through  
Enterprise Risk Management”***

(Draft as in Sep-2019)

**A Framework for driving better privacy  
engineering and help organizations  
protect individuals’ privacy by-**

- ❖ building customer trust;
- ❖ fulfilling compliance obligation;
- ❖ facilitating communication on privacy;  
and practice with stakeholders.

# Download our publications



## Ethical Accountability Framework for Hong Kong, China

A Report prepared for the Office of the Privacy Commissioner for Personal Data

*Analysis and Model Assessment Framework*



## 香港個人資料私隱專員公署簡介

About the Office of the Privacy Commissioner for Personal Data, Hong Kong

[PCPD.org.hk](http://PCPD.org.hk)

Protect, Respect Personal Data  
維護 - 尊重個人資料



## 私隱管理系統 Privacy Management Programme 最佳行事方式指引 A Best Practice Guide

2018年9月  
August 2018



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



# Contact Us



## Copyright



- Hotline 2827 2827
- Fax 2877 7026
- Website [www.pcpd.org.hk](http://www.pcpd.org.hk)
- E-mail [enquiry@pcpd.org.hk](mailto:enquiry@pcpd.org.hk)
- Address 1303, 13/F, Sunlight Tower,  
248 Queen's Road East,  
Wanchai, HK

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](http://creativecommons.org/licenses/by/4.0).