

Hong Kong Academy of Law

5 June 2019

# Privacy Protection and Data Governance in the Internet of Things

Stephen Kai-yi Wong, Barrister

Privacy Commissioner for Personal Data, Hong Kong, China

1

PCPD



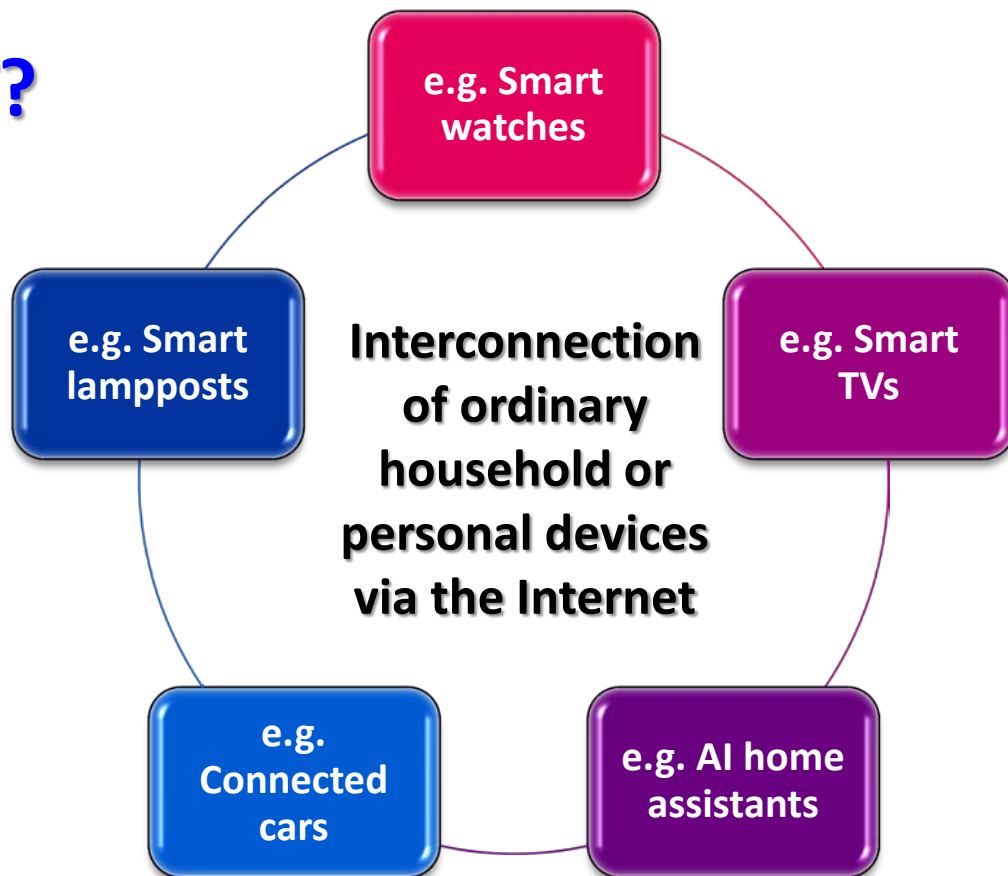
HK



PCPD.org.hk

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

# What is IoT?



**Wi-Fi  
Connected City**



**Intelligent  
Transport System  
and Traffic  
Management**

**eID**



**Big Data Analytics  
Platform**

**FinTech**



# Hong Kong Smart City Initiatives



**Smart Tourism**

**Multi-functional  
Smart Lampposts**



**Open Data**

**Digital Payment**



3

Source: Hong Kong Smart City Blueprint

PCPD



PCPD.org.hk

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

# Wi-Fi Connected City



## Intelligent Transport System and Traffic Management

A diagram showing a hand holding a smartphone with various transport icons (bus, car, train, etc.) connected to a central point, with a Wi-Fi signal icon at the top.

## eID

An illustration of a hand holding a smartphone displaying a digital ID card.

## Big Data Analytics Platform

A hexagonal icon containing a cloud with data bars and a server rack below it.

## FinTech

A close-up of a keyboard with a blue key labeled 'FINTECH' and a dollar sign icon.

# Smart city initiatives that may involve IoT & digital tracking

A photograph of a man and a woman looking at a smartphone together, with icons for a shopping bag and a location pin overlaid.

## Smart Tourism

## Multi-functional Smart Lampposts

A diagram of a smart lamppost with icons for Wi-Fi, CO2, and other sensors.

## Open Data

A hexagonal icon with various symbols including a graduation cap, a stethoscope, a location pin, a cloud, and a train.

## Digital Payment

A photograph of a hand holding a smartphone over a payment terminal.

# IoT may involve one or more of the following technologies...

Examples of applications:

- Intelligent traffic signal
- Real-time parking vacancy system
- Smart lamppost
- Autonomous vehicle

Electronic sensor

RFID / NFC

Examples of applications:

- Mobile payment
- Electronic baggage tag
- Auto toll
- Electronic road pricing

Example of application:

- Almost everything

Wi-Fi / Mobile network

Webcam

Examples of applications:

- Real-time traffic information
- Electronic road pricing
- Smart lamppost
- Autonomous vehicle

Example of application:

- Autonomous vehicle

Audio recording

iBeacon

Examples of applications:

- Crowd management
- Smart lamppost

5



# Whether the data collected by IoT is “personal data”?

## Definition of “personal data” under the PD(P)O



(a) Relating directly or indirectly to a living individual



(b) Practicable for the identity of the individual to be directly or indirectly ascertained; and



(c) In a form in which access to or processing is practicable

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

# Whether the data collected by IoT is “personal data”?



ability to collect a vast amount of intimate information concerning an individual’s health, movements, habits and private life



piecing together information gathered via different IoT devices → allow a profile be constructed of the IoT user



tracking of an IoT device may be tantamount to behavioural tracking of the user

## Whether the data collected by IoT is “personal data”?



The US Court of Appeal for the Seventh Circuit

*Naperville Smart Meter Awareness v.*

*City of Naperville*, No. 16-3766  
(7th Cir. 2018)

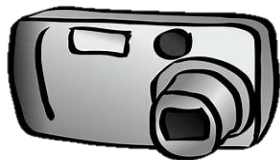
energy consumption data of a household collected by a smart energy meter

protected by the Fourth Amendment to the US Constitution (i.e. the right of people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures)

the energy usage data revealed information about the happenings inside the house



# Meaning of “collect” as defined in *Eastweek* case applicable in the context of IoT?



## The *Eastweek* case



A  
complaint  
lodged  
with the  
PCPD in  
1997

The complainant  
was photographed  
by a magazine  
without her  
knowledge or  
consent

The photograph  
published in the  
magazine  
accompanied by  
unflattering and  
critical comments on  
her dressing style

# Revisit the Meaning of “collect” as defined in *Eastweek* case in the context of IoT?

## The *Eastweek* case

PCPD: contravened  
DPP 1(2)(b)

Court of Appeal:  
No “collection” of  
personal data by the  
publisher

Court of First  
Instance for judicial review:  
Application dismissed

10

# Revisit the Meaning of “collect” as defined in *Eastweek* case in the context of IoT?

Businesses may track individuals' online activities with cookies and slowly build up profiles to send targeted marketing messages to their computers - may not have identified or intend to identify the individuals in the first place

**Initially:** May be completely indifferent to and ignorant of the identities of the individuals being tracked

**Subsequently:** May identify individuals and reveal details of their intimate lives by applying techniques of big data analytics and profiling

Application of the *Eastweek* case places extra burden on the individuals and regulators to prove the intent of the businesses

If a person installs CCTVs merely for monitoring the surroundings, in the absence of “collection”, the PDPO will not come into play. Amassing databases of CCTVs' images increases risks of privacy harms from data mishandling or breaches

Big data analytics and AI algorithms mostly function to predict trends to inform businesses' decisions, as opposed to identifying individuals. If general privacy principles do not apply as a result of not meeting the conditions of “collect” → may undermine protection to the troves of data collected and stored in the event of data security incidents

# Privacy Risks of IoT

An IoT device (e.g., webcam, iBeacon) may track, monitor and collect data from *any persons* coming within its monitoring area

**Undistinguished and excessive collection**  
(cf. DPP 1)

**Covert tracking and monitoring; no meaningful notice and consent**  
[cf. DPPs 1 & 3]

**Vulnerable to security breach**  
(DPP 4)

**Privacy Risks**

Individuals may be unaware of the tracking and monitoring devices (e.g. RFID, webcam, iBeacon)

IoT devices may lack security measures (e.g., firewall, anti-virus software, end-to-end encryption)

12

# Case sharing: Unsecure Webcams (2016)



South China Morning Post HK CHINA ASIA WORLD COMMENT BUSINESS TECH LIFE CULTURE SPORT WEEK IN ASIA POST MAG STYLE

SHARE

NOW READING

Prying webcams used by artist to capture unsuspecting Hongkongers in controversial

## Prying webcams used by artist to capture unsuspecting Hongkongers in controversial UK exhibition

Privacy experts have criticised a London artist for unfairly accessing peoples' personal data after home devices were used without consent to collect images from inside homes

PUBLISHED : Tuesday, 16 August, 2016, 2:03am  
UPDATED : Wednesday, 17 August, 2016, 7:48pm

COMMENTS: 3



Source:

<https://www.scmp.com/news/hong-kong/law-crime/article/2004219/prying-webcams-used-artist-capture-unsuspecting-hongkongers>

13

PCPD



PCPD.org.hk

HK

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



# Case sharing: IoT Toys (2017)



News > Business > Business News

## Your child's doll could be spying on them, privacy group warns

Two internet-connected toys have been called out by consumer protection groups for turning over data collected from conversations with children to companies without permission

Zlata Rodionova | Monday 12 December 2016 13:51 | 6 comments

f t e Like Click to follow The Independent Online

Vivid Toys and Games



Source: <https://www.independent.co.uk/news/business/news/my-friend-cayla-i-que-intelligent-robot-genesis-smart-toys-spying-on-children-a7469741.html>


South China Morning Post HK CHINA ASIA WORLD COMMENT BUSINESS TECH LIFE CULTURE SPORT WEEK IN ASIA POST MAG STYLE

SHARE f t e + NOW READING Amazon and Toys R Us urged to withdraw toys that allow hackers to exploit Bluetooth

## Amazon and Toys R Us urged to withdraw toys that allow hackers to exploit Bluetooth flaw to talk to children

Which? investigation finds security flaws in 'intelligent' toys such as CloudPets and Hasbro's Furby Connect

PUBLISHED : Tuesday, 14 November, 2017, 12:20pm  
UPDATED : Tuesday, 14 November, 2017, 9:24pm



Source: <https://www.scmp.com/news/world/article/2119790/amazon-and-toys-r-us-urged-withdraw-toys-allow-hackers-exploit-bluetooth>

14



Wi-Fi  
Connected City



eID



FinTech



**Smart city initiatives that may involve  
open data & big data analytics**



Smart Tourism

Multi-functional  
Smart Lampposts



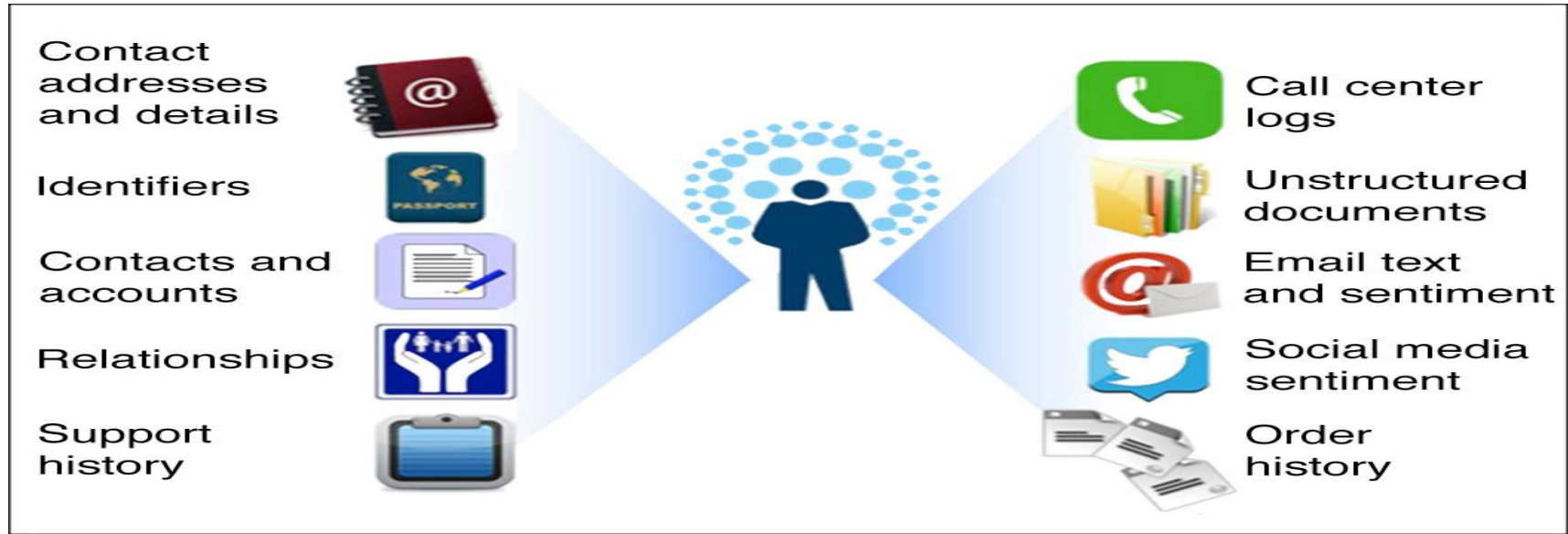
Open Data

Digital Payment



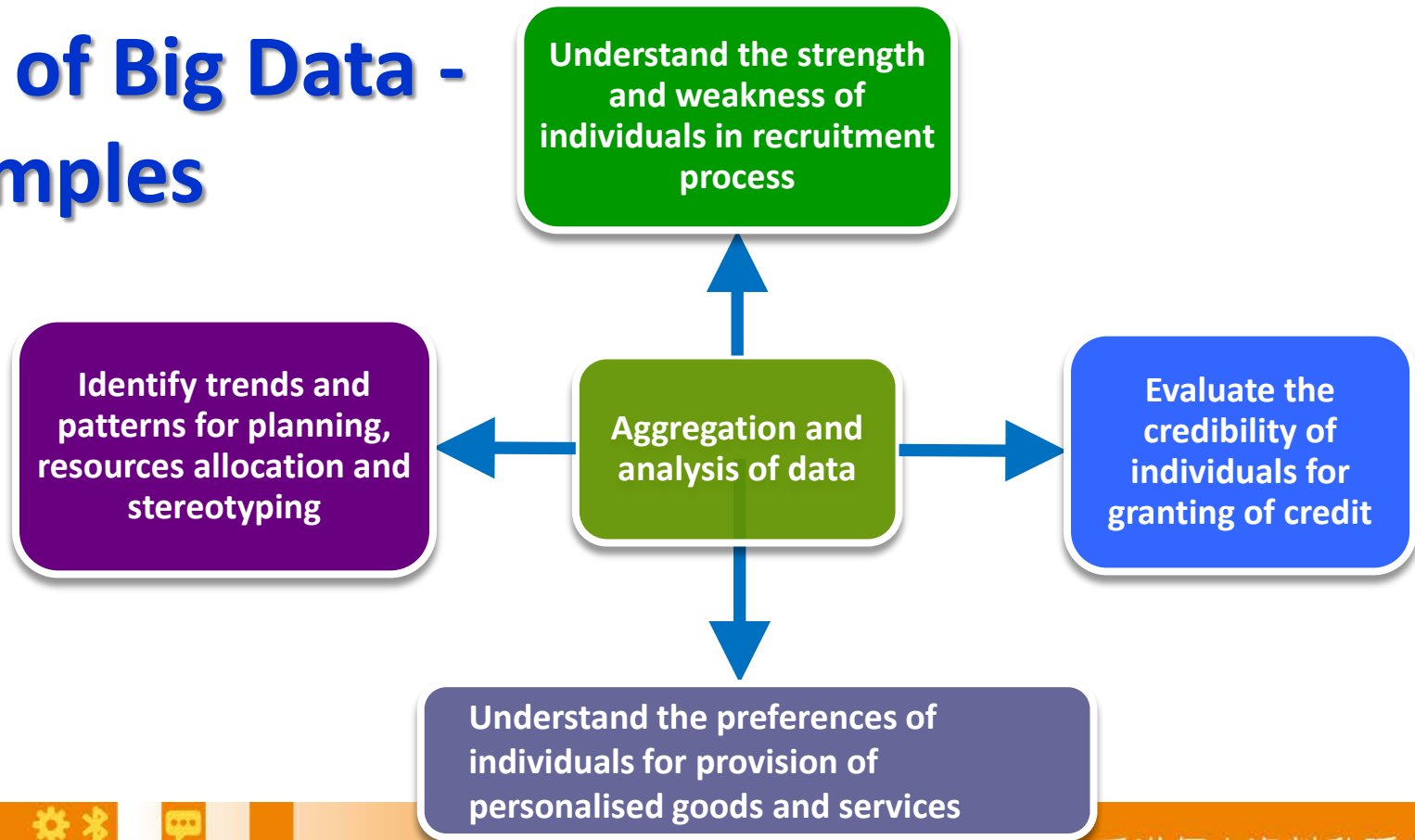
# Big Data

**Massive scale of collection, processing, combination and aggregation of structured & unstructured data**



16

# Use of Big Data - Examples



# Privacy risks associated with open data and big data analytics

## Open data / Big data analytics

- **Re-identification** of individuals from anonymous data by big data analytics [*cf. DPP 1 (fair collection)*]
- Revelation of **personal secrets** by big data analytics [*cf. DPP 1 (fair collection)*]
- Mistaking coincidence / correlation as causality → **bias / unfair discrimination** [*DPP 2 (accuracy)*]
- Sharing and use of personal data beyond individuals' **reasonable expectations** [*cf. DPP 3*]
- Lack of **transparency** (unexplainable algorithms) [*cf. DPP 5*]

18

## Netflix Cancels Contest Plans and Settles Suit

BY STEVE LOHR MARCH 12, 2010 2:46 PM 41

Netflix's \$1 million prize contest was such a research and business hit that when the winners were declared last September the company immediately announced plans for another one.

But it turned out that letting very smart computer scientists and statisticians dig through the video rental site's data had one major, unforeseen, drawback. A pair of researchers at the University of Texas showed that the supposedly anonymized data released for the contest, which included movie recommendations and choices made by hundreds of thousands of customers, could in fact be used to identify them.

Source: [https://bits.blogs.nytimes.com/2010/03/12/netflix-cancels-contest-plans-and-settles-suit/?\\_r=0](https://bits.blogs.nytimes.com/2010/03/12/netflix-cancels-contest-plans-and-settles-suit/?_r=0)

19

PCPD



HK



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



# How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did



Kashmir Hill, FORBES STAFF  
Welcome to The Not-So Private Parts where technology & privacy collide FULL BIO

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target TGT -1.03%, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Charles Duhigg outlines in the *New York Times* how Target tries to hook parents-to-be at that crucial moment before they turn into rampant -- and loyal -- buyers of all things pastel, plastic, and miniature. He talked to Target statistician Andrew Pole -- before Target freaked out and cut off all communications -- about the clues to a customer's impending bundle of joy. Target assigns every customer a Guest ID number, tied to their credit card, name, or email address that becomes a bucket that stores a history of everything they've bought and any demographic information Target has collected from them or bought from other sources. Using that, Pole looked at historical buying data for all the ladies who had signed up for Target baby registries in the past. From the NYT:

“ [Pole] ran test after test, analyzing the data, and before long some useful patterns emerged. Lotions, for example. Lots of people buy lotion, but one of Pole's colleagues noticed that women on the baby registry were buying larger quantities of unscented lotion around the beginning of their second trimester. Another analyst noted that sometime in the first 20 weeks, pregnant women loaded up on supplements like calcium, magnesium and zinc. Many shoppers purchase soap and cotton balls, but when someone suddenly starts buying lots of scent-free soap and extra-big bags of cotton balls, in addition to hand sanitizers and washcloths, it signals they could be getting close to their delivery date.



Target has got you in its aim [-]

Source:

<https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#2d7cf09a6668>

20

PCPD



PCPD.org.hk

H K

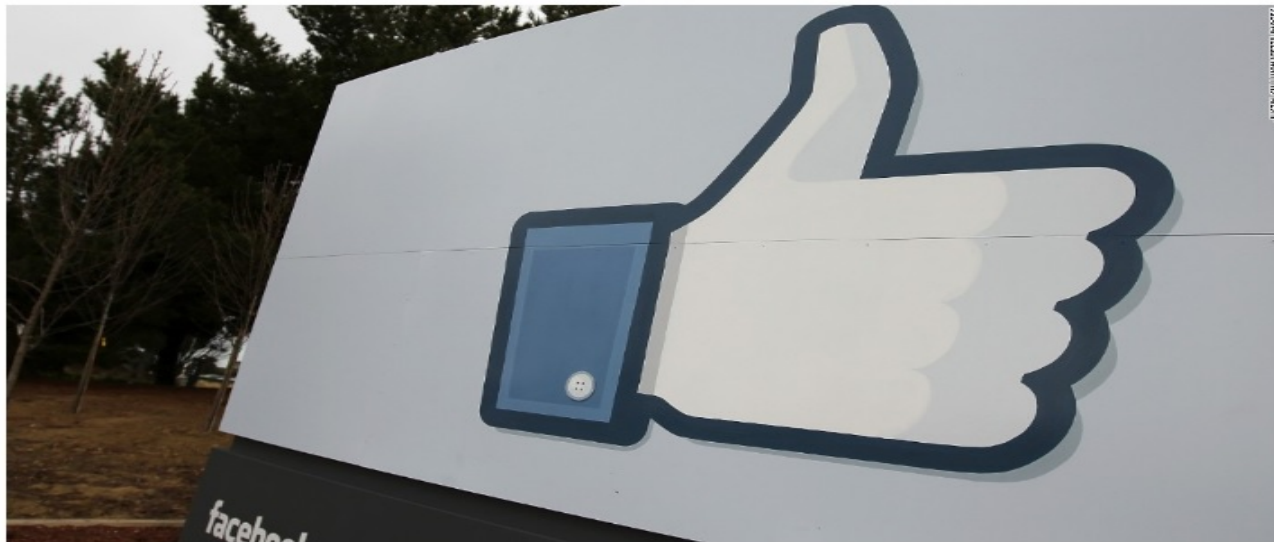
香港個人資料私隱專員公署  
Privacy Commissioner  
for Personal Data, Hong Kong



# Facebook 'likes' can reveal your secrets, study finds

By Heather Kelly, CNN

🕒 Updated 1900 GMT (0300 HKT) March 11, 2013



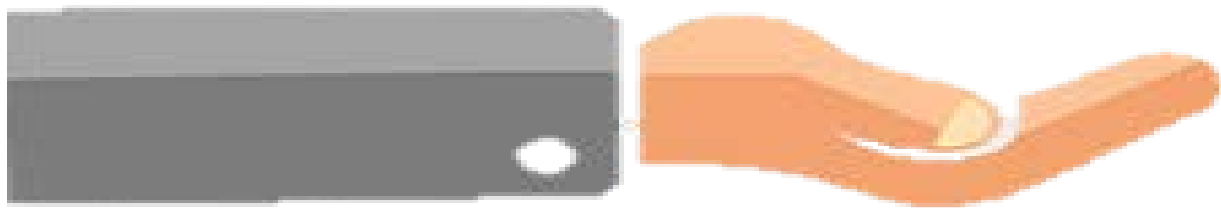
A new study claims it is possible to predict personal information about a person just by analyzing their Facebook likes.

Source:

<https://edition.cnn.com/2013/03/11/tech/social-media/facebook-likes-study/>

21

# *Trust is indispensable*



# Create Trust in Smart City Initiatives and IoT

## Transparency

Provide privacy policies in plain and concise language



## Accountability

Adopt Privacy Management Programme

- Privacy Impact Assessment
- “Privacy by Design” and “Privacy by Default”

Minimise collection of personal data

Adopt commensurable security measures to protect data in transit and in storage

23

**Our customers' trust  
means everything to us.  
We spent decades  
working to earn that  
TRUST.**

*Tim Cook, 2015*



***Our data is being  
weaponised against us.***

*Tim Cook, 2018*



**Trust is the new gold.**

**Andrea Jelinek**  
**Chair of European Data Protection Board**



25

PCPD



HK



PCPD.org.hk

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

# Least Common Multiple (LCM) approach: Accountability & Ethics



*“Arguably the biggest change [brought by the GDPR] is around **accountability.**”*

Elizabeth Denham, Information Commissioner of the UK

*“[The GDPR] aims to **restore a sense of trust and control** over what happens to our online lives.”*

Giovanni Buttarelli, European Data Protection Supervisor

26



# Accountability and Governance

## EU GDPR

**Risk-based approach to accountability.** Data controllers are required to:

- implement **technical and organisational measures** to ensure compliance [Art 24];
- adopt **data protection by design and by default** [Art 25];
- conduct **data protection impact assessment** for high-risk processing [Art 35]; and
- (for certain types of organisations) **designate Data Protection Officers** [Art 37].

## HK PDPO

The accountability principle and the related privacy management tools are not explicitly stated.

The Privacy Commissioner advocates the **Privacy Management Programme** which manifests the accountability principle. The appointment of data protection officers and the conduct of privacy impact assessment are recommended good practices for achieving accountability.

# Accountability: Privacy Management Programme (PMP)



Effective management of personal data



Minimisation of privacy risks



Effective handling of data breach incidents



Demonstrate compliance and accountability

Download >>



# PMP – Main Components



## 1. Organisational Commitment

1.1 Buy-in from the Top ...

1.2 Appointment of Data Protection Officer/  
Establishment of Data Protection Office ...

1.3 Establishment of Reporting Mechanisms

29

# PMP – Main Components



## 2. Programme Controls

2.1 Personal Data Inventory



2.2 Internal Policies on  
Personal Data Handling



2.3 Risk Assessment Tools

2.4 Training, Education and  
Promotion



2.5 Handling of Data  
Breach Incident

2.6 Data Processor  
Management



2.7 Communication

30

# PMP – Main Components



## 3. Ongoing Assessment and Revision

3.1 Development of an Oversight and Review Plan

...

3.2 Assessment and Revision of Programme Controls

31



# Ethics and Trust





# Ethics as a Bridge between Law and Expectation

- Business model and technological development vis-a-vis legislation and regulatory reform
- Public expectation forever increasing
- How to bridge the gap?
- Data Ethics

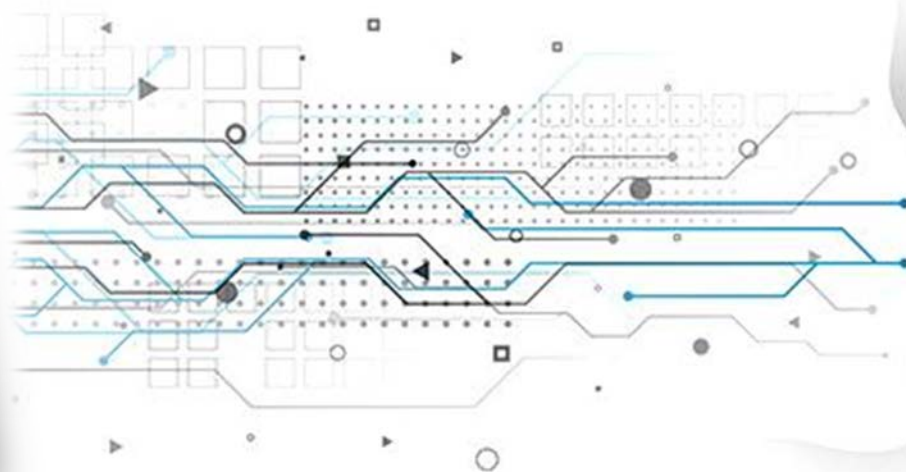
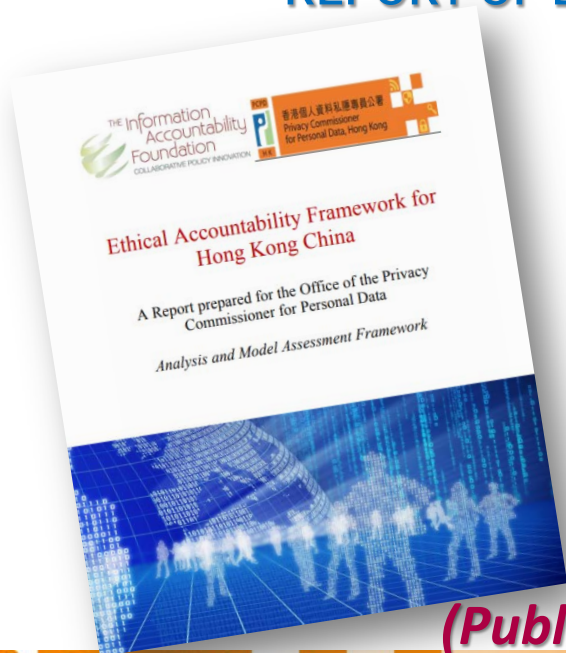


# Fair Enforcement

Ethics

# “Ethical Accountability Framework for Hong Kong China”

## REPORT OF LEGITIMACY OF DATA PROCESSING PROJECT



*(Published on 24 October 2018)*

Download >>

35

PCPD

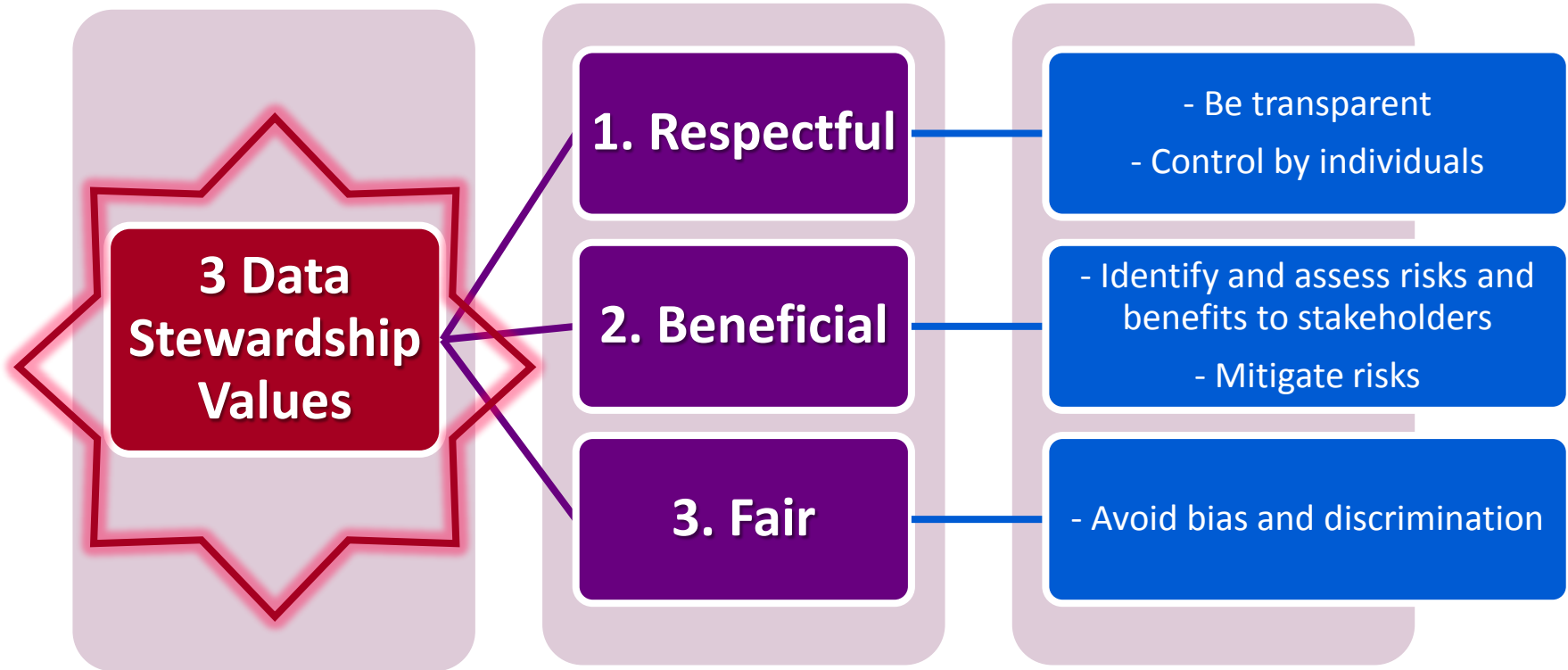


PCPD.org.hk

H K

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

# Multi-stakeholders' Approach – Three Core Values



36

# Multi-stakeholders' Approach – Two Assessment Models

## 2 Assessment Models

1. Model Ethical Data Impact Assessment

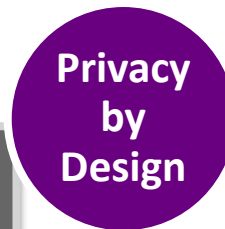
2. Process Oversight Model

Assess the impact of data processing activities on all stakeholders

Evaluating organisations' data stewardship



# Data Ethics - Implementation



**Step 1: Analyse the business objective and purpose of the data processing activity**

**Step 2: Assess the nature, source, accuracy and governance of the data**

**Step 3: Conduct impact assessment, i.e. risks and benefits to the individuals, the society and the organisation itself**

**Step 4: Balance between expected benefits and the mitigated risks to all stakeholders**

# Process Oversight – Questions to Consider

Are the **accountability and responsibility** of data stewardship clearly defined?

Are the core values translated into **principles, policies and processes**?

Does the organisation adopt “**ethics by design**”?

Are **Ethical Data Impact Assessments** properly conducted?

Are **internal reviews** conducted periodically?

Are there any **feedback and appeal mechanisms** for the individuals impacted ?

Is there any mechanism to ensure the **transparency** of the data processing activities?

# Data Ethics



Think, plan and execute with multi-stakeholders' interests

Get data management on a cradle-to-grave basis in an institutional system and process

Review the system and process regularly



Data Ethics

40

# Examples of Privacy by Design and by Default



Under iOS 12.2, access to location data of iPhone or iPad by website operators is disabled by default

- To allow websites to their access location data, users have to switch on the function themselves, providing users with stronger control

Source: Ars Technica; Feb 2019

41

# Examples of Privacy by Design and by Default



About the ICO / News and events / News and blogs /

## ICO fines Uber £385,000 over data protection failings

Date 27 November 2018  
Type News

The Information Commissioner's Office (ICO) has [fined ride sharing company Uber £385,000](#) for failing to protect customers' personal information during a cyber attack.

A series of avoidable data security flaws allowed the personal details of around 2.7million UK customers to be accessed and downloaded by attackers from a cloud-based storage system operated by Uber's US parent company. This included full names, email addresses and phone numbers.

The records of almost 82,000 drivers based in the UK – which included details of journeys made and how much they were paid – were also taken during the incident in October and November 2016.

The ICO investigation found 'credential stuffing', a process by which compromised username and password pairs are injected into websites until they are matched to an existing account, was used to gain access to Uber's data storage.

Also paid \$148 million  
in U.S.

- Uber changes its privacy settings after having been fined
  - ❖ 'hiding precise pickup and dropoff locations' in the driver app after a trip ends to help protect information about rider locations
  - ❖ riders and drivers can call or chat with each other directly in the Uber app, so rider no need to share their phone number

Source: ICO; Nov 2018

42



# Examples of Ethics by Design

For personalised online advertising and marketing\*\*:

- make it clear to the consumers if a recommendation of goods/services is a personalised advertisement; and
- provide consumers with information about other similar but non-personalised goods/services.

\*\* Reference: draft revision to the Personal Information Security Specification of China (Jan-2019)



Reference:  
PCPD's Information Leaflet



## Physical Tracking and Monitoring Through Electronic Devices

[https://www.pcpd.org.hk//english/resources\\_centre/publications/files/physical\\_tracking\\_e.pdf](https://www.pcpd.org.hk//english/resources_centre/publications/files/physical_tracking_e.pdf)

# Design & Development of IoT Devices

## Manufacturers of IoT devices should:

- provide privacy policies in plain language;
- inform users the types of personal data to be collected, the purposes of collection, the potential transferees of the personal data and the security measures;
- minimise data collection, incorporate sufficient security safeguards and adopt the least privacy-intrusive default settings;
- offer opt-out choice to users for the access to the data that is not relevant to the main purpose of the IoT devices;
- give clear instructions to users on how to delete their personal data stored;
- provide users with contact information for pursuing privacy-related matters.



# Use of RFID



## Manufacturers that would incorporate RFIDs in their products should:

- clearly inform consumers that RFID tags are used and embedded in products;
- offer options to consumers to disable or remove the RFID tags;
- avoid storing personal data in RFID tags;
- shield the information in the RFID tags from being read by unauthorised parties;
- avoid containing readable unique identification numbers in RFID tags;
- select the read range of RFID tags with due consideration to privacy and data protection.



# Case Sharing: RFID Baggage Handling System

Privacy concerns are properly reduced by...

1

Storing minimal data in baggage tags & baggage handling system

2

Restricting airline's access to its own passengers' data for baggage reconciliation purposes only

3

Not transferring passengers' data outside the system



47

PCPD



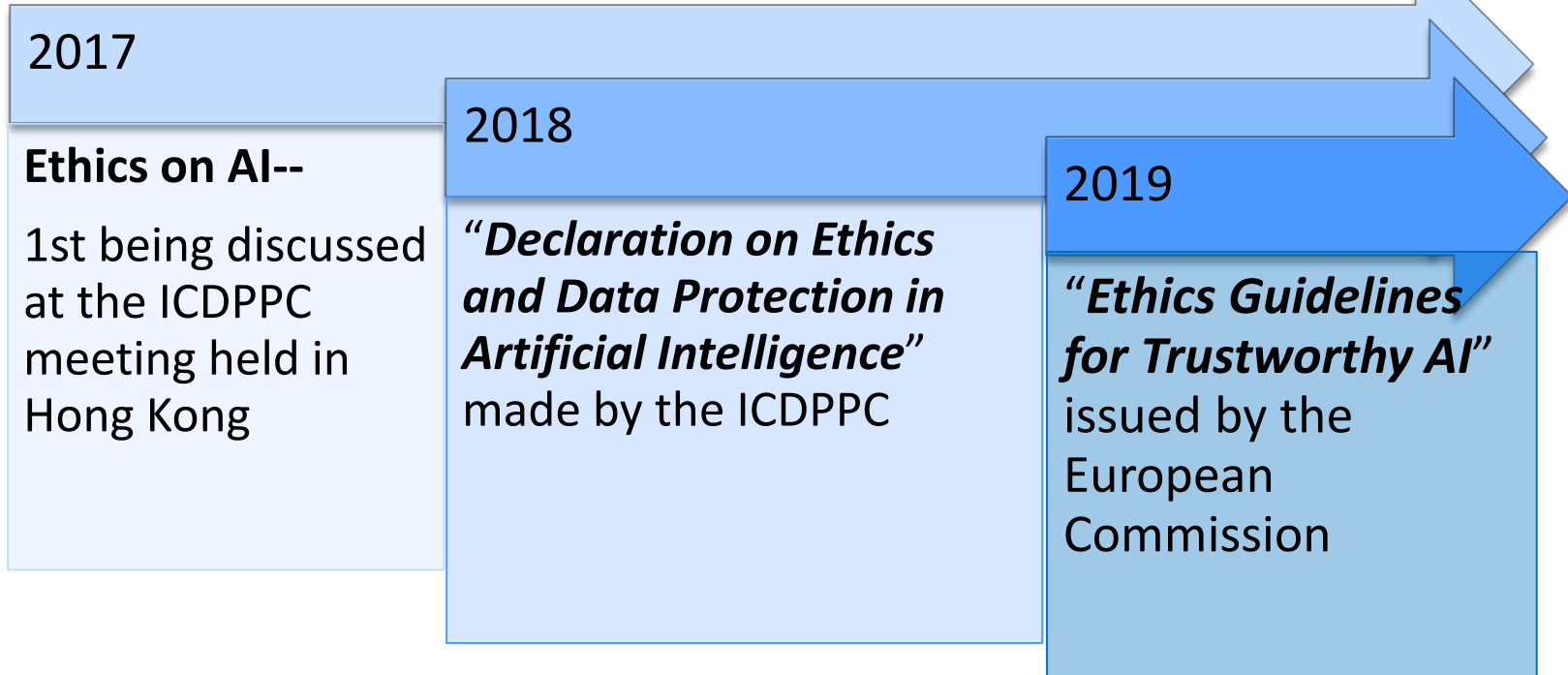
HK

PCPD.org.hk

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



# Data Ethics-Global Landscape



# “Declaration on Ethics and Data Protection in Artificial Intelligence” made by the 40th ICDPPC



Respect of the rights to privacy and data protection are increasingly challenged by the development of AI

Risks of malicious use of AI, and potential risks related to privacy, data protection and human dignity induced by AI

Inherent bias contained in data sets used to train AI systems

Strong data protection and privacy safeguards help to build individuals' trust in how their data is processed, which encourages data sharing and thereby promotes innovation

# Treat Data as Money



## Money

- (1) Accountant
- (2) Accounting rules
- (3) Money ledger
- (4) Reporting
- (5) Board meetings

## Data

- (1) Data Protection Officer
- (2) Data protection policy and guidelines
- (3) Personal Data Inventory
- (4) Compliance reporting and monitoring
- (5) Board commitment

**New!**



Issued by the PCPD in April 2019

Aims to help SMEs understand the means to implement data ethics

[https://www.pcpd.org.hk//english/resources\\_centre/publications/files/dataethics\\_en.pdf](https://www.pcpd.org.hk//english/resources_centre/publications/files/dataethics_en.pdf)

52

PCPD



H.K.

PCPD.org.hk

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



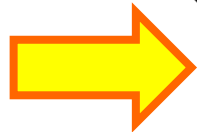
# PCPD's Roles – Enforcer + Educator + Facilitator

## PCPD's Strategic Focus

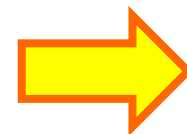
Fair Enforcement



Engaging

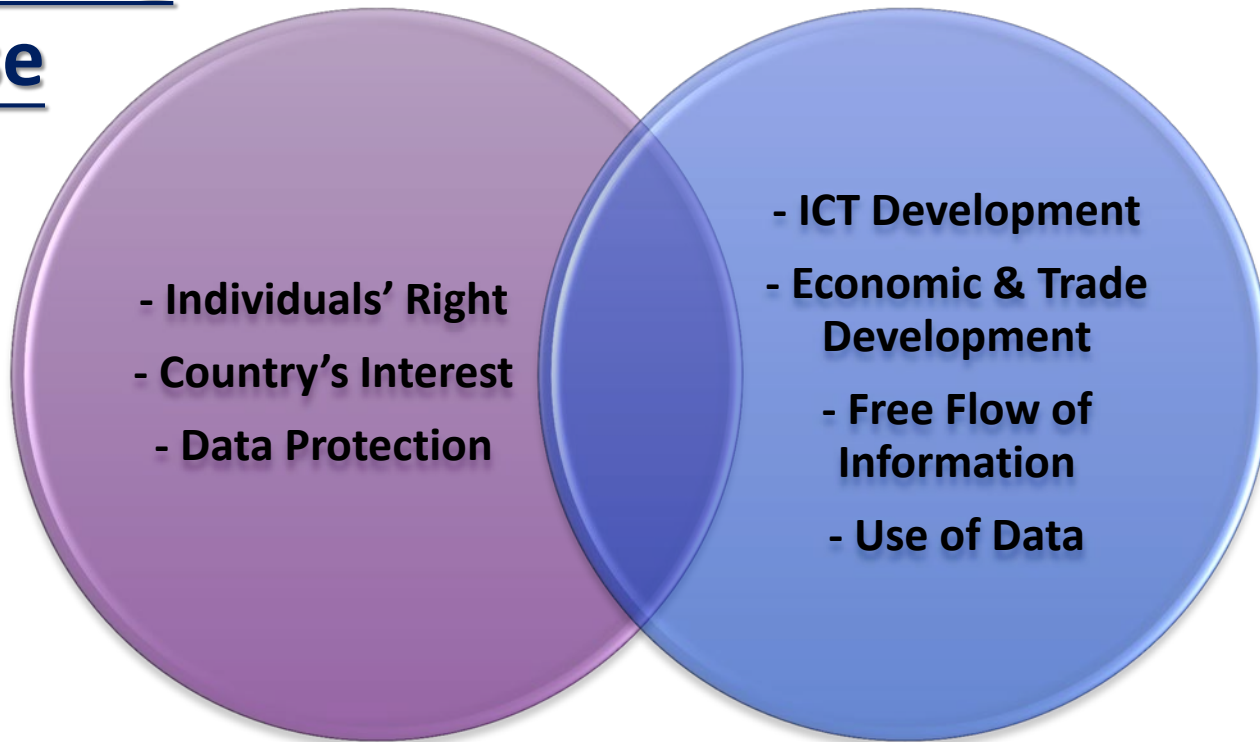


Incentivising



Privacy-friendly Culture

# A Balancing Exercise





## HKMA's circular on 3 May 2019

- To all authorized institutions
- Encourages them to adopt and implement the Ethical Accountability Framework in the development of fintech products and services

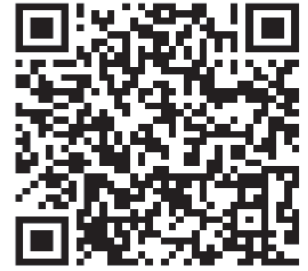
<https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190503e1.pdf>

# Q&A

# Thank you

## "Ethical Accountability Framework for Hong Kong, China"

REPORT OF LEGITIMACY OF DATA PROCESSING PROJECT



## Legitimacy of Data Processing Project Media Statement



## Data Ethics for Small and Medium Enterprises

### Preamble

In a data-driven economy, small and medium enterprises ("SMEs"), including tech startups, increasingly use personal data of customers to assist in operating and advancing their business. The rapid development of information and communications technology, particularly advanced data processing, artificial intelligence, big data analytics and other intelligent information technologies has at the same time challenged privacy and data protection.

It is not to dispute that personal data belongs to the data subjects. While that does not mean that personal data should stick to the strict of individual's requests to exercise their data protection rights, SMEs should consider all parties that have access to the data.

In fact, ethical use of personal data makes good business sense. **Responsible, beneficial** and fair use of customers' personal data can improve business reputation and enhance stakeholders' confidence. This guide serves to help SMEs understand the means

practical personalisation and modulation in the future smart market integration and trends by grasping and implementing data ethics.

### Three Core Values of Data Ethics

SMEs are encouraged to handle personal data pursuant to these core values, namely, being **Responsible, Beneficial** and **Fair**.

#### Responsible

- SMEs should be accountable for conducting ethical data processing activities.
- SMEs should consider the expectations of the individuals to whom the data refers and/or impacted by the data use.
- SMEs should consider all parties that have access to the data.
- Decisions made about an individual and the impact decision-making process should be explainable and reasonable.
- Individuals should be able to make inquiries, obtain registration and appeal against decisions on the advanced data processing activities that impact them.





# Contact Us



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

58

☐ 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

PCPD



HK

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

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