

Zürich Meets Hong Kong – A Festival Of Two Cities
The Future of Privacy Symposium
26 October 2017

Observations on the GDPR 2018
from Hong Kong's Perspective

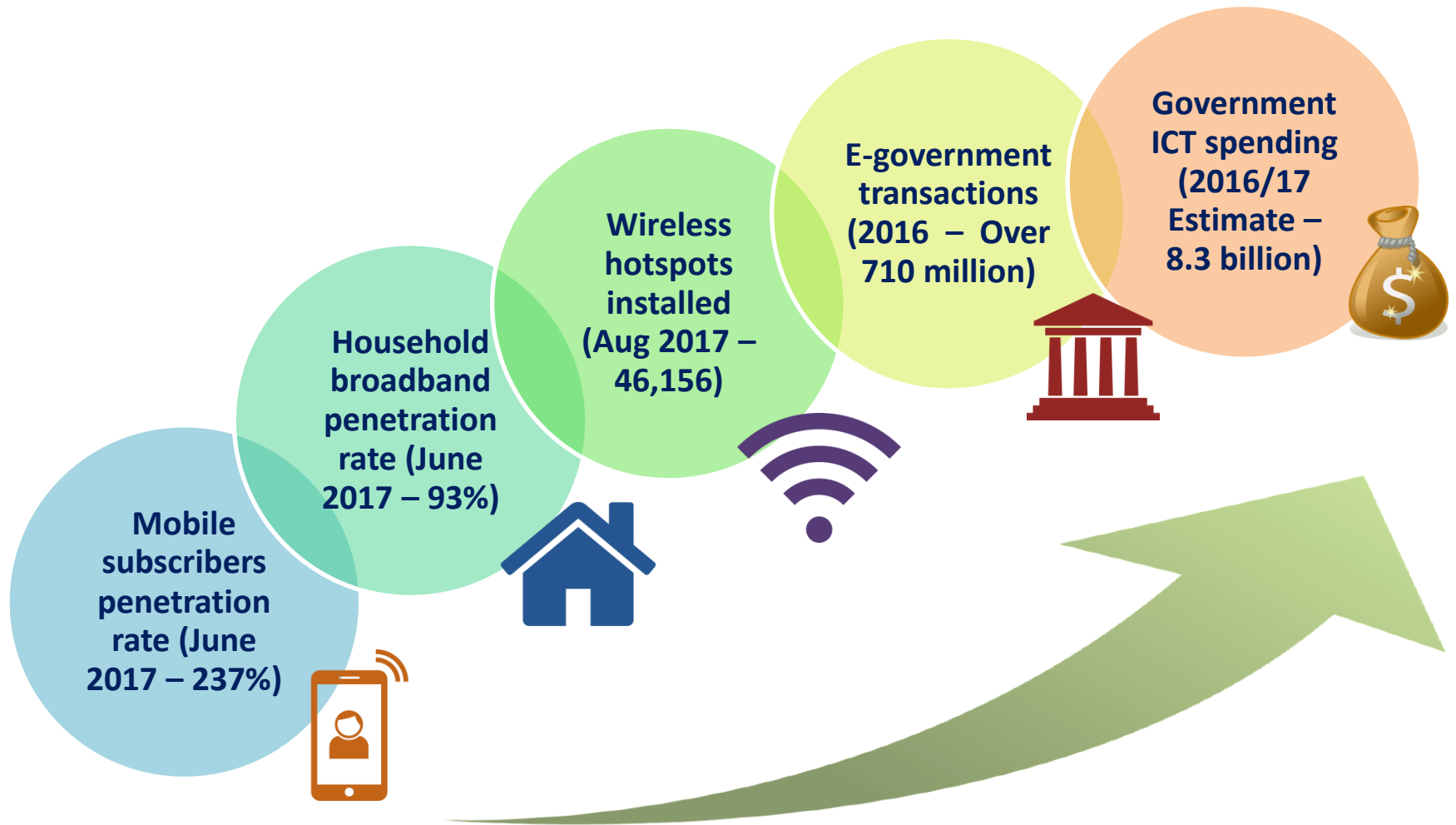
保護・尊重個人資料
Protect, Respect Personal Data

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

Recent Changes in Data Protection Landscape

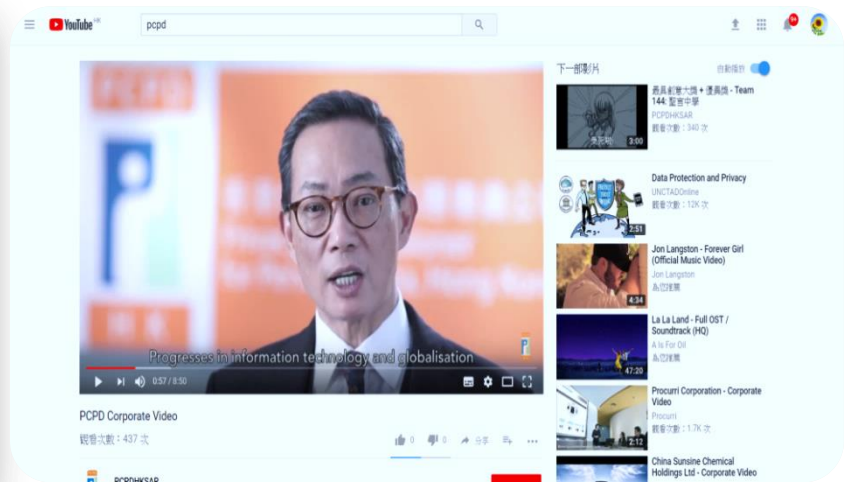


Hong Kong Going Digital



Source: Hong Kong Government Digital 21 Strategy – Statistics and Figures

Hong Kong – Digital Craze



Mainland of China – QR Code?



Mainland of China – QR Code?

“WeChat + Begging”



Social Media



Facebook Claims 5 Million Monthly Users in Hong Kong



Facebook claims 5 million monthly users in HK

Wednesday, September 28, 2016

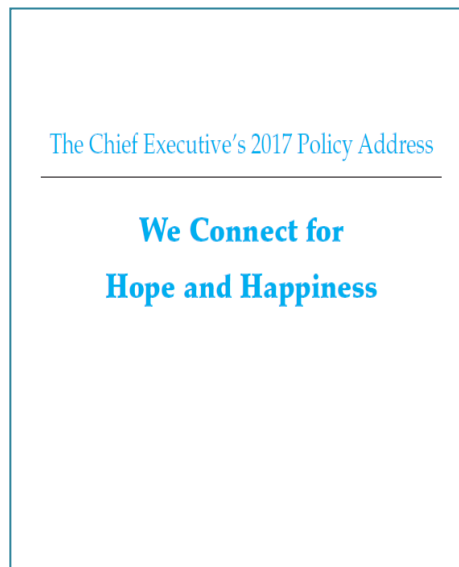
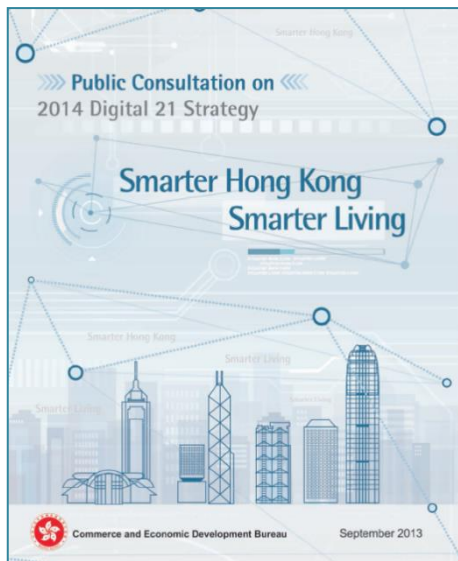
Facebook announced it has 5 million monthly active users, of which 4.6 million are mobile monthly active users in Hong Kong.

According to the company it also has more than 4 million businesses in world that advertise on Facebook, with more than 70 percent outside of the United States.

Source: The Standard, 28 Sept 2016

8

Hong Kong – Smart City



- 2014 Digital 21 Strategy
- Smart Hong Kong Consultancy Study Report 2017
- The Chief Executive's 2017 Policy Address

Privacy Issues in the Age of Big Data, Artificial Intelligence & Internet of Things

- Covert Data Collection
- Tracking and Monitoring
- Re-identification
- Profiling
- Cybersecurity...



10



and Its Impact on Hong Kong

11



PDPO – GDPR Comparative Study

Background

- **Keep abreast with overseas'** privacy law developments
- Assess GDPR's **impact on businesses** (in particular multi-national organisations)
- Comparable legal framework facilitates **free flow of information** and commercial activities



PDPO – GDPR Comparative Study

PCPD identified the following 9 major differences between PDPO and GDPR:

9 Major Differences	
1. Extra-Territorial Application	6. Data Processor Obligations
2. Accountability and Governance	7. New or Enhanced Rights of Data Subjects/Profiling
3. Mandatory Breach Notification	8. Certification/Seals and Personal Data Transferred Outside Jurisdictions
4. Sensitive Personal Data	9. Sanctions
5. Consent	

1. Extra-Territorial Application

EU GDPR

Data processors or controllers:

- with an establishment in the EU, or
- **established outside the EU**, that offer goods or services to individuals in the EU, or monitor the behaviour of individuals in the EU. [Art 3]

HK PDPO

Data users who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the personal data **in or from Hong Kong**. [S.2(1)]



2. 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.

3. Mandatory Breach Notification



EU GDPR

- Data controllers are required to **notify the authority** about a data breach without undue delay (**exceptions** apply).
- Data controllers are required to **notify affected data subjects unless exempted**.
[Arts 33-34]

HK PDPO

- No mandatory requirement.
Voluntary breach notification.

4. Sensitive Personal Data

EU GDPR

- Expand the category of sensitive personal data.
- Processing of sensitive personal data is allowed only under specific circumstances. [Art 9]

HK PDPO

- No distinction between sensitive and non-sensitive personal data.



5. Consent

EU GDPR

- One of the 6 lawful bases for processing
- Consent must be
 - ✓ **freely given, specific and informed**; and
 - ✓ **an unambiguous indication of a data subject's wishes**, by statement or by clear affirmative action, which signifies agreement to the processing of his personal data. [Art 4(1)]

HK PDPO

Consent is not a pre-requisite for the collection of personal data, unless the personal data is used for a new purpose. [DPPs 1&3]



6. Data Processor Obligations

EU GDPR

- Data processors are imposed with additional obligations, such as: **maintaining records of processing, ensuring security of processing, reporting data breaches, designating Data Protection Officers, etc.**
[Arts 30, 32-33, 37]

HK PDPO

- Data processors are **not directly regulated.**
- Data users are required to **adopt contractual or other means to ensure data processors comply with data retention and security requirements.** [DPPs 2&4]



7. New or Enhanced Rights of Data Subjects / Profiling

EU GDPR

- Right to **erasure of personal data** (also known as “right to be forgotten”) [Art 17]
- Right to **data portability** [Art 20]
- **Right to object to processing** (including profiling) [Art 21]
- **“Profiling”** is defined as any form of automated processing involving personal data to evaluate certain personal aspects of a natural person [Art 4(4)]
- Expanded notice requirement for the new or enhanced rights

HK PDPO

- No general right to erasure, but shall not retain personal data for longer than necessary [S.26 & DPP 2(2)]
- No right to data portability
- No general right to object to processing (including profiling), but may **opt out from direct marketing activities** [Ss.35G &35L] and contains provisions regulating data matching procedure [Ss. 30-31]

8. Certification / Seals and Personal Data Transferred Outside Jurisdictions

EU GDPR

- Explicitly recognises privacy seals and establishes **certification mechanism** for demonstrating compliance by data controllers and processors. [Art 42]
- Certification as **one of the legal bases for cross-border data transfer.**

HK PDPO

- No such certification or privacy seals mechanism for demonstrating compliance.



9. Sanctions



EU GDPR

- Data protection authorities can impose **administrative fines** on data controllers and processors. [Art 58]
- Depending on the nature of the breach, the fine could be up to **€20million** or **4%** of the total worldwide annual turnover. [Art 83]

HK PDPO

- The Privacy Commissioner is not empowered to impose administrative fines or penalties.
- The Privacy Commissioner may serve **enforcement notices** on data users.



PDPO – GDPR Comparative Study





Observations – Notice & Consent

- **Balance** with genuine needs for processing data
- Over reliance on consent may **impede** business activities
- PDPO is principle-based and **technology neutral**
- Suggest stick to DPP1 & DPP3:
 - **DPP1** – notice; lawful purpose directly related to a function or activity
 - **DPP3** – use for new purpose not allowed without prescribed consent



Observations – Accountability

- **Suggest formalising accountability principle (including mandatory DPO regime) under PDPO because it can:**
 - give effect to principle-based PDPO by promoting responsible use of data by data users
 - facilitate compliance
 - allow for more flexibility to tackle the challenges brought by ICT, AI, Big Data, etc.
- **To mitigate adverse effect on businesses, risk-based approach to accountability can be considered**
- **PCPD is open-minded as to formalising PIA as it is already a part of PMP**



Observations – Sanctions

- Allow PCPD to impose administrative fines would **deter non-compliance** and bring PDPO in line with overseas data protection laws (e.g. Singapore, UK)
- **Some regulators in Hong Kong are also vested with power** to order pecuniary penalty, e.g. Monetary Authority, Securities and Futures Commission
- **Appropriate check & balance mechanism** may allay concerns of over-concentration of powers:
 - i. stipulating criteria for imposing fines
 - ii. prescribing fine limit
 - iii. allowing appeal channel against fine imposed



Observations – Extra-Territorial Application

- Given rapid ICT developments, data collection and processing nowadays is borderless. **Currently, PCPD will resort to cross-border enforcement where appropriate**
- Adopting extra-territoriality to PDPO requires consideration of **complicated legal issues**, practicality of enforcement and consistency with international comity
- PCPD has reservation on making same change to PDPO
- It is **still an open question to be clarified by legal precedent** as to whether PDPO has extra-territorial effect

Way forward

- **Publication of Guidance**
- **Trainings for data users**
- **Information exchange and experience sharing on issues and challenges relating to compliance with GDPR**
- **Strengthen international cooperation**



Q&A

Contact Us

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

保護・尊重個人資料
Protect/Respect Personal Data

About PCPD | Data Privacy Law | News & Events | Compliance & Enforcement | Complaints | Legal Assistance | Education & Training | Resources Centre | Enquiry

A Quick Guide

Hot Search | Advanced Search | Keyword Search

What's New

PCPD Wins the "Most Breastfeed-caring Corporate" Award

PCPD's New Chinese Publication Entitled 《注意！這是我的個人資料私隱》 has been released at the Hong Kong Book Fair 2017! The new book sharing session was held at the HKCEC on 24 July 2017.

PCPD Publishes a New Book Entitled "Watch out! This is my personal data privacy" - Have a Say on Your Own Privacy! (Chinese version Only)

Privacy Commissioner Welcomes the Enactment of the Apology Ordinance

Organisations and Individuals Should Comply with Lawful Requirement of the Privacy Commissioner - A Company Director Became the First Offender Convicted of this Offence

Privacy Commissioner Publishes Investigation Report on the Loss of Registration and Electoral Office's Notebook Computers containing Personal Data of Election Committee Members and Electors

PCPD Joins Global Sweep Exercise to Examine Consumers' Control Over Their Personal Data Collected by Customer Loyalty and Reward Programmes

"It is a timely opportunity for Hong Kong to review the data privacy protection law" Privacy Commissioner Delivers Keynote Address at the 7th European Data Protection Days in Berlin, Germany

For Individuals

Think Privacy! Be Smart Online
Using Computers and the Internet Wisely
Be Smart on Social Networks
Your Identity Card Number and

For Organisations

Mobile App Development
Professional Workshops
Online Courses
Introduction to the PD(P)O Seminar

The 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC)

The 39th International Conference of Data Protection and Privacy Commissioners is now open for registration.

- ☐ Hotline 2827 2827
- ☐ Fax 2877 7026
- ☐ Website www.pcpd.org.hk
- ☐ E-mail enquiry@pcpd.org.hk
- ☐ Address 12/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.

спасибо
 danke 謝謝
 ngiyabonga
 teşekkür ederim
 tapadh leat
 dank je
 gracias
 mochchakkeram
 bedankt
 hvala
 maururu
 thank you
 go raibh maith agat
 dziekuje
 sagolun
 sukriya
 kop khun krap
 arigato
 takk
 dakujem
 merci
 obrigado
 unjofes
 sukriya
 terima kasih
 감사합니다
 ευχαριστώ
 grazie