The Hong Kong General Chamber of Commerce
Digital, Information and Telecommunication Committee
11 December 2017

Recent Developments of Privacy Laws in the Mainland of China and EU

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

Presentation Outline

- China's Cybersecurity Law
- Other latest developments in the mainland of China
- EU General Data Protection Regulation (GDPR) 2018

Data Protection Laws in mainland of China

1. No omnibus data protection law
2. Piecemeal regulations, mainly relates to use of information technology (e.g., regulations for mobile apps and social media)
3. Lack of comprehensive protection to personal data privacy

China's Cybersecurity Law

China's Cybersecurity Law

- effective on 1 June 2017

- Purposes: [Art 1]
  - guarantee cybersecurity
  - safeguard cyberspace sovereignty
  - safeguard national security and public interest
  - protect lawful rights and interests of citizens, legal persons and other organisations
  - promote sound development of economic and social informatisation (信息化)

China's Cybersecurity Law

Scope of Application:

- apply to the construction, operation, maintenance and use of the network, and the supervision and administration of cybersecurity within China [Art 2]
- mainly regulate network operators, i.e. the owners and administrators of the network as well as network service providers. [Art 76(3)]
    - not limited to technology companies e.g. a financial institute which uses computer network in its operation is a network operator
- protect personal information

China's Cybersecurity Law - Requirements

Data Collection & Use:

- where personal information is collected, **notify** users and obtain their **consent** [Art 22]
- follow principles of **legality**, **rightfulness** and **necessity** during collection and use; explicitly indicate the **purposes, means** and **scope** of collection and use [Art 41]
- **do not collect** personal information irrelevant to services provided [Art 41]
- **do not collect or use** personal information in violation of any law or administrative regulation or agreement of both parties [Art 41]

China's Cybersecurity Law - Requirements

Data Accuracy & Record Retention:

- not tamper with personal information collected [Art 42]

- take technical measures to monitor and record the status of network operation and cybersecurity incidents, and preserve weblogs for not less than 6 months [Art 21(3)]

China's Cybersecurity Law - Requirements

Data Security & Breach Notification:

- strictly keep confidential users' personal information collected, and establish and improve the system for information protection [Art 40]

- do not damage personal information collected, and take technical measures and other necessary measures to ensure security of personal information collected, and prevent information leakage, damage and loss [Art 42]

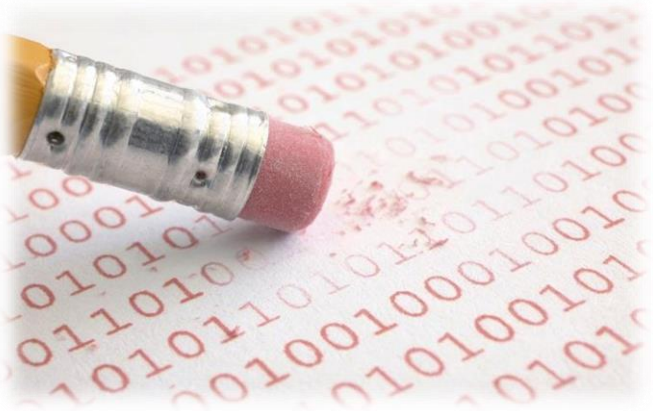
- where personal information has been or is likely to be divulged, damaged or lost, take remedial measures, inform users, and report to regulatory authority [Art 42]

China's Cybersecurity Law - Requirements

Data Deletion & Correction:

- individual can request network operator to **correct** his personal information collected or stored if there is any **error** [Art 43]

- individual can request network operator to **delete** his personal information, if the operator collects or uses information in **violation** of any law, administrative regulation or agreement of both parties [Art 43]



China's Cybersecurity Law - Requirements

Data Localisation:

- **personal information and important data collected and produced by operators of critical information infrastructure (CII) during their operations within China shall be stored within China [Art 37]**

- **if CII operators need to provide such information and data to overseas parties due to business requirements, they shall conduct security assessment according to the measures developed by the Cyberspace Administration of China (CAC) and relevant departments of State Council, unless otherwise prescribed [Art 37]**

- **other network operators are encouraged to voluntarily participate in the CII protection system [Art 31]**

China's Cybersecurity Law - Requirements

Data Localisation:

- **CII examples: public communications and information services, energy, transport, water conservancy, finance, public services, e-government affairs, and CII that will result in serious damage to state security, national economy and people's livelihood and public interest if it is destroyed, loses functions or encounters data leakage [Art 31]**

China's Cybersecurity Law - Sanctions

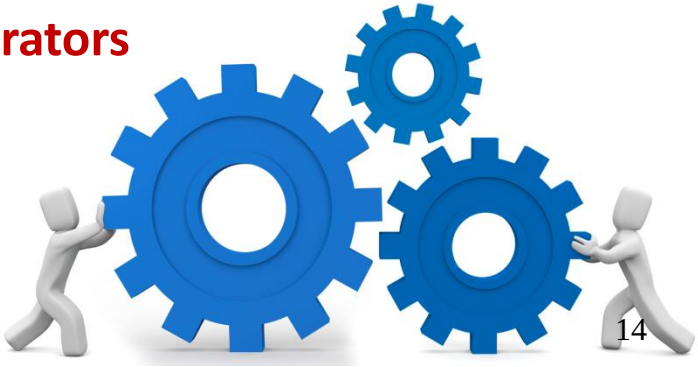
Possible sanctions for a breach:

- corrective action
- warning
- confiscate illegal income,
- fine between 1 and 10 times of illegal income
- if no illegal income, impose fine < RMB 1 million
- impose fine between RMB 10,000 and 100,000 on directly responsible person
- in serious cases, suspend or cease business operation for rectification, or close down website, or revoke business permit or license [Arts 64 & 66]

[Depending on the graveness of the case, the above sanctions may be applied simultaneously]

"Measures for Security Assessment of Cross-Border Transfer of Personal Information and Important Data"
《個人信息和重要數據出境安全評估辦法》

- Purposes: Elaborate the requirements of security assessment for cross-border data transfer under the Cybersecurity Law
- Draft Measures first issued in April 2017, and revised in May 2017
- Final version of the Measure is not yet available
- According to the latest draft, all network operators (not only CII operators) should conduct security assessment before transfer of personal information and important data to a place outside mainland of China



"Guidelines for Data Cross-Border Transfer Security Assessment"
《數據出境安全評估指南》

- **Purposes: Provide substantive guidance on how to perform security assessment for transfer of personal information and important data to a place outside mainland of China**
- **Latest draft of the Guidelines issued on 31 August 2017**
- **Final version of the Guidelines is not yet available**
- **Clarify the operations by:**
  - providing definition of domestic operation and data cross-border transfer
  - elaborating self-security assessment process
  - specifying the conditions, process and requirements of government assessments

The New York Times | https://nyti.ms/2vbooTd

BUSINESS DAY

Apple Opening Data Center in China to Comply With Cybersecurity Law

点击查看本文中文版

By PAUL MOZUR, DAISUKE WAKABAYASHI and NICK WINGFIELD JULY 12, 2017

SHANGHAI — Apple said Wednesday that it would open its first data center in China, joining a parade of technology companies responding to growing global demands to build facilities that store online data closer to customers.

The move is a response to a strict new law in China that requires companies to store users' data in the country. The new data center, in Guizhou, a province in southwest China, is part of a $1 billion investment in the province and will be operated in partnership with a local data management company, Apple said.

The move is part of a worldwide trend regarding the security and sovereignty of digital data. Microsoft, Amazon and Facebook are among the big American technology companies plowing billions of dollars into building data centers in Germany, the Netherlands, France and other countries. While some of the expansion is for technical reasons — the online services operate faster when they are near customers — the companies are also reacting to growing pressure from European governments and customers to maintain some control over their data.

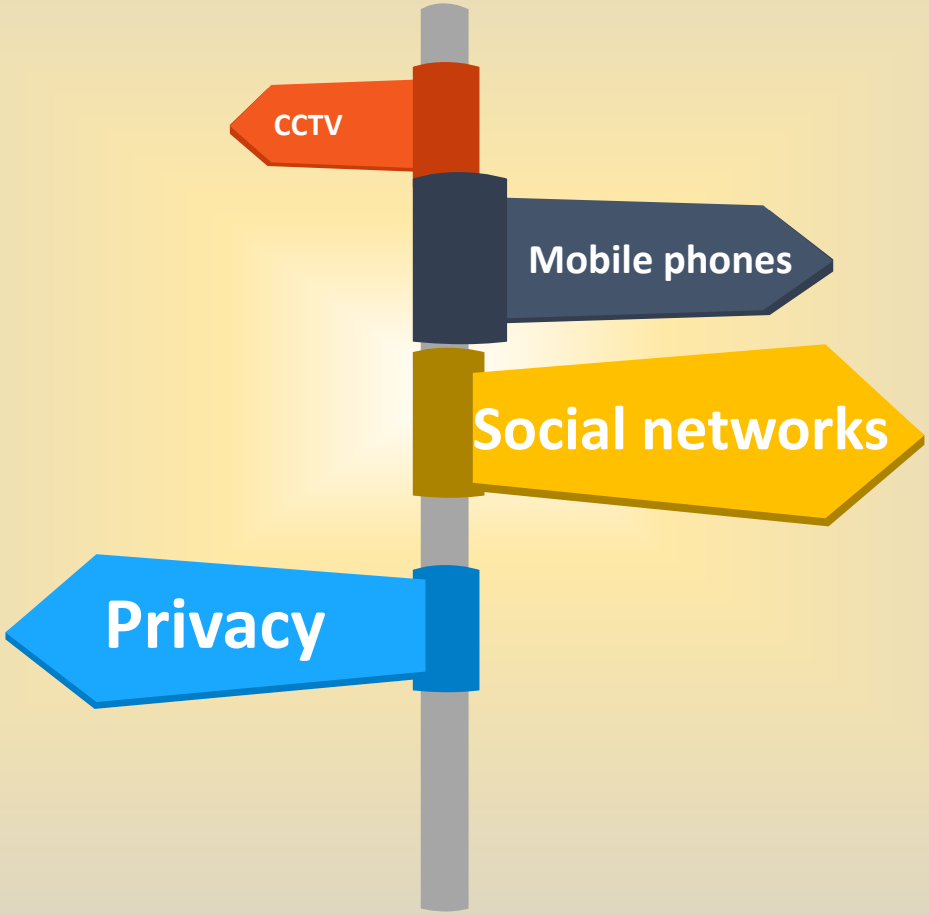
As is the case with many laws, the digital security regulations approved last month in China were vaguely worded, leaving many foreign companies uncertain about which parts would be enforced and how. Already, Amazon, Microsoft and IBM have formed partnerships with Chinese companies to offer cloud computing services

https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html?mkt_tok=eyJpIjoiTTJaak16STFOR1V6WW1RMyIsInQiOiIz... 1/4

Apple Opening Data Centre in China to Comply With Cybersecurity Law

Source: The New York Times 12 July 2017

Other Recent Development in Mainland China



The Interpretation of Various Issues Concerning Application of Law in Handling Crimes of Infringing upon Citizen's Personal Data
《關於辦理侵犯公民個人信息刑事案件適用法律若干問題的解釋》

Jointly issued by the PRC Supreme People's Court and the Supreme People's Procuratorate in May 2017

Clarifying and expanding the definition of personal information for the purpose of the Criminal Law

- **personal information means any information, individually or combined with other information, that can identify a specific individual**
- **new examples include account password, financial position and geo-location data**

Make it clear that it is a crime to publicise personal information without consent

- **publication of personal information through the Internet or other channels without consent fall within the crime of infringement of personal information under the Criminal Law, even if the information is legally obtained** *(partly for addressing the increasing trend of "cyber manhunt" （人肉搜索）)*

Court Judgment on the use of CCTV

Oct 2017: The People's Court of Changning District, Shanghai City (上海市長寧區人民法院)

Ordered the defendants, who had installed a CCTV camera at the entrance of their residence, to dismantle the CCTV

The Court considered that the privacy of the other people passing the public walkway would also be intruded

Major Impact of the EU GDPR

EU General Data Protection Regulation (GDPR)

- approved by EU Parliament on 14 April 2016
- will be enforced on 25 May 2018
- replaces the 1995 EU Data Protection Directive (95/46/EC)
- harmonises data protection laws across EU

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	HK PDPO
Regulate both data processors and controllers that: • with an establishment in the EU, or • established outside the EU, but offer goods or services to individuals in the EU, or monitor the behaviour of individuals in the EU [Art 3]	**Regulate only 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	HK PDPO
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]** • **(for certain types of organisations) designate Data Protection Officers [Art 37]**	**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	HK PDPO
• 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]	• No mandatory requirement • Voluntary breach notification

4. Sensitive Personal Data

EU GDPR	HK PDPO
• Expand the category of sensitive personal data to include genetic data, biometric data and sexual orientation • Processing of sensitive personal data is allowed only under specific circumstances (e.g., explicit consent) [Art 9]	• No distinction between sensitive and non-sensitive personal data. 

5. Consent

EU GDPR	HK PDPO
• 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)]	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	HK PDPO
• Data processors are imposed with additional obligations, such as: ▪ maintaining records of processing ▪ ensuring security of processing ▪ reporting data breaches ▪ designating Data Protection Officers [Arts 30, 32-33, 37]	• 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	HK PDPO
• 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	• 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]

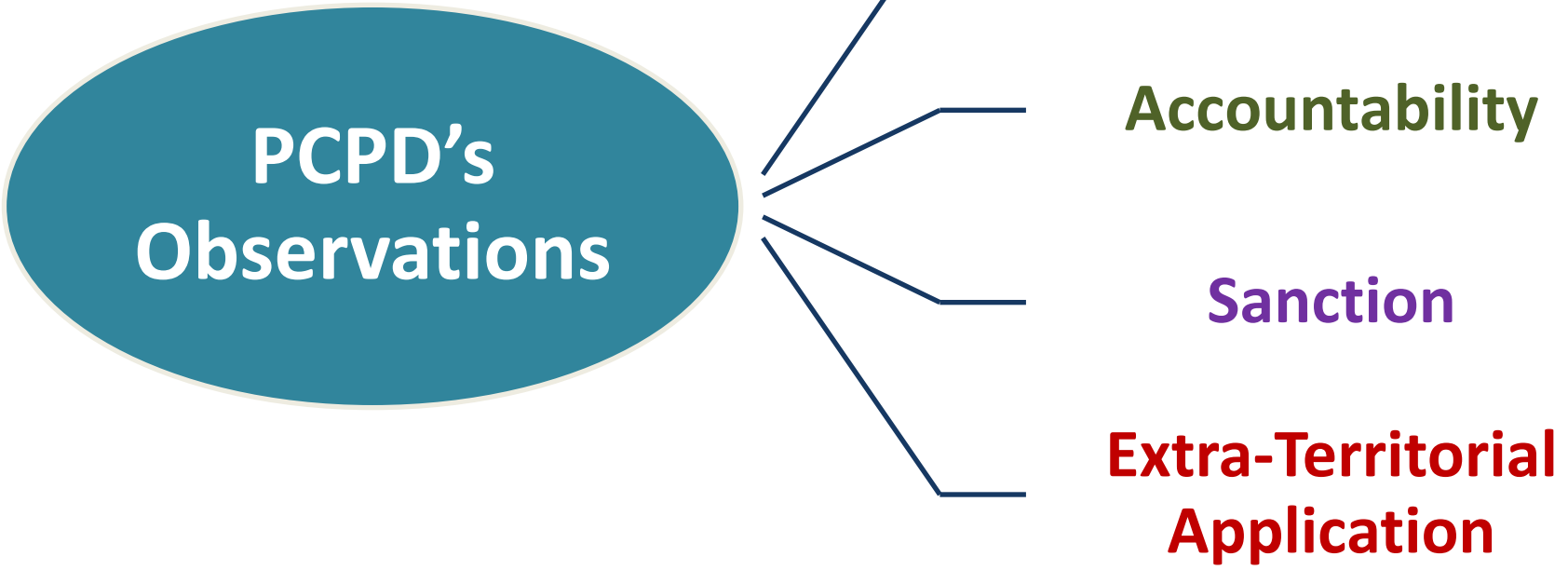
8. Certification / Seals and Personal Data Transferred Outside Jurisdictions

EU GDPR	HK PDPO
• 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**	• No such certification or privacy seals mechanism for demonstrating compliance 

9. Sanctions

EU GDPR	HK PDPO
• Data protection authorities can impose **administrative fines** on data controllers and processors [Art 58]	• The Privacy Commissioner is not empowered to impose administrative fines or penalties.
• Depending on the nature of the breach, the fine could be up to **€20million** or **4%** of the total worldwide annual turnover [Art 83]	• The Privacy Commissioner may serve **enforcement notices** on data users.

PDPO – GDPR Comparative Study



Observations – Notice & Consent

- **Consent approach** gives effect to individual autonomy
- Over reliance on consent may **impede** business activities and shift the burden of personal data protection to individuals
- PDPO is principle-based and **technology neutral**
- Suggest stick to DPP1 & DPP3:
  - **DPP1** – collect personal data only for lawful purpose directly related to a function or activity; provide notice
  - **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, e.g., IoT, AI, Big Data
- 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 cooperation 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 organisations**
- **Information exchange and experience sharing on issues and challenges relating to compliance with GDPR**
- **Strengthen international cooperation**

Contact Us

- ❑ **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