

China Cybersecurity Law Conference:
New Legal and Regulatory Updates
Practical Implications and Challenges

The Changing Personal Information Regulatory Framework in the Mainland of China

11 December 2019 | 12/F Sunlight Tower, 248 Queen's Road East, Hong Kong

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

PCPD



PCPD.org.hk

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

Mainland of China

Major Milestones of Personal Information / Data / No Privacy

551 BC

- Johnny Kung – Confucianism – 五倫 (5 principles of inter-personal relationship)

1949

- People's Republic of China

1966 – 1976

- Cultural Revolution

1979

- My first footprints in the Mainland

1992

- Deng inspection trip in Shenzhen (Modernisation of China)

2019

- 31% world's mobile data traffic

China punishes 100 apps for breaches of personal information as consumer anxiety rises over privacy

- The China Cybersecurity Center said 100 apps, across a range of industries including e-commerce and banking, have been penalised since November



Celia Chen

Published: 12:42pm, 9 Dec, 2019



Source: SCMP; 9 Dec 2019

- Continuous crack down of apps by authorities amid rising consumer anxiety
- Malpractices include:
 - incorrect collection of personal information
 - lack of policies or ambiguous rules
- **Enforcement actions:**
 - 27 of the apps received rectification orders
 - 63 received written warnings
 - 10 were issued with fines
 - 2 were under criminal investigation

Development of ICT: Big Data, Cloud Computing, AI, etc.



Constitutional Guarantee

- Personal dignity of Chinese citizens is inviolable
- Unlawful search of or entry into the homes of citizens is prohibited
- Freedom and secrecy of citizens' communications shall be protected by law

[\[Constitution of China, Articles 38 – 40\]](#)

Privacy & Data Protection in mainland China



Criminal Law

9th Amendment (2015):
Criminalises obtaining personal information by theft or other unlawful means, and for the sale or sharing of personal information in violation of relevant national regulations.

[\[Criminal Law, Article 253\(1\)\]](#)

The Supreme People's Court and the Supreme People's Procuratorate's interpretation on 'Personal Information'

Personal Information

*“all kinds of information in electronic or other recorded format that can be used to **independently identify or be combined with other information to identify** a natural person, or to **provide indications** of the activities of a specific natural person.”*

→ Wider than the definition of “personal data” under PDPO

e.g. location and movement information

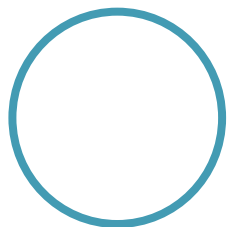
Criminal Law Provisions

9th Amendment (2015):

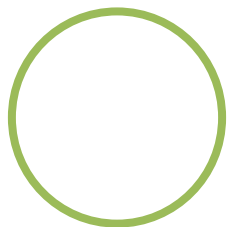
Criminalises obtaining personal information by theft or other unlawful means, and for the sale or sharing of personal information in violation of relevant national regulations.

[Criminal Law, Article 253(1)]

Mainland China 's Data Protection Regime

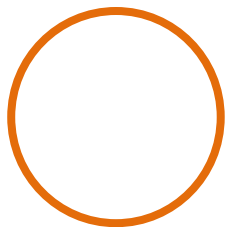


No comprehensive piece of legislation specifically directed at the protection of personal information currently



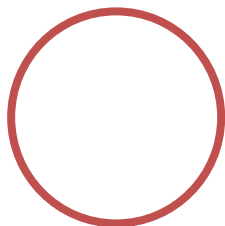
Has an assortment of normative instruments touching on protection of personal information – e.g. laws, administrative regulations, departmental rules and guidelines

Mainland China 's Data Protection Regime



No dedicated authority with vested responsibility for enforcement of privacy and data protection laws

Law enforcement agencies include:



- Cyberspace Administration of China (CAC)
- Ministry of Industry and Information Technology (MIIT)
- Ministry of Public Security (if crime is involved)
- Other industry regulators

China is stepping up personal information protection

Springing up of laws and regulations on personal information protection

Starting recognising privacy and personal information protection as civil rights

Strengthening personal data and privacy protection using criminal enforcement and administrative actions

Draft comprehensive personal data protection law planned to submit to Congress by March 2023

Chronology of data protection regulations

《侵權責任法》
Tort Law



Implemented: Jul 2010

《刑法修正案（九）》
**Criminal Law
(9th Amendment)**



Implemented: Mar 2014



Implemented: Nov 2015

**Law on Protection
of Consumer Rights
and Interests
(2nd Amendment)**

《消費者權益保護法》
第二次修正

**Provisions on
Administration of Mobile
Internet Applications
Information Services**

《移動互聯網應用程序信息服務管理規定》

《網絡安全法》
**Cybersecurity
Law**



Implemented: Aug 2016



Implemented: Jun 2017

Chronology of data protection regulations

《民法總則》
General Provisions of the Civil Law



Implemented: Oct 2017

《個人信息安全規範》
Personal Information Security Specification (1st Edition)



Implemented: Jun 2017



Implemented: May 2018



Implemented: Jan 2019

《兒童個人信息網絡保護規定》
Provisions on Cyber Protection of Children's Personal Information



Implemented: Oct 2019

Interpretations of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in the Handling of Criminal Cases of Infringing on Citizens' Personal Information

E-Commerce Law

《電子商務法》

《最高人民法院 最高人民檢察院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》

Other draft regulations in the pipeline

- **Administrative Measures for Data Security** 《數據安全管理辦法》
- **Measures for the Security Assessment for Cross-border Transfer of Personal Information** 《個人信息出境安全評估辦法》
- **Personal Information Security Specification** 《個人信息安全規範》 (2nd Edition)
- **Basic Specification for Collecting Personal Information in Mobile Internet Applications** 《移動互聯網應用（App）收集個人信息基本規範》
- **Civil Code: Part on Personality Right** 《民法典人格權編》

Brief introduction of...

Cybersecurity Law

The overarching legislation in data protection

Related administrative regulations

Administrative Measures for Data Security (Consultation Draft)

Measures for Security Assessment for Cross-border Transfer of Personal Information (Consultation Draft)

Provisions on Cyber Protection of Children's Personal Information

Personal Information Security Specification (Draft – 2nd Edition)

Administrative Measures for Disclosure of Cybersecurity Threats (Consultation Draft)

13

1. Cybersecurity Law

- Came into force in **June 2017**
- Regulate “**network operators**”

“Network operator”: the owner or administrator of a network, or the provider of network services.

Almost all entities which use network in their operations are caught.



How may Cybersecurity Law affect Hong Kong businesses?



- Processing of personal data by a Hong Kong-based business is regulated by Hong Kong's Personal Data (Privacy) Ordinance, but not Mainland's Cybersecurity Law

Unless

Then

- The processing also involves construction, operation, maintenance or use of networks in the mainland of China

- Both the Personal Data (Privacy) Ordinance and the Cybersecurity Law may apply to the processing activities



- CLC has no explicit extraterritoriality
- But be wary of collecting personal information from individuals in mainland

15

1. Cybersecurity Law: requirements

Cybersecurity Law
– Articles 40 - 42

Personal information protection principles:

- a) Personal information must remain **confidential**, protected by a **comprehensive and robust system**
- b) Collection and use of personal information must be **necessary, lawful and proper**
- c) **Rules and policy** concerned with collection and processing of personal information must be **disclosed**
- d) **Purpose, method and scope of collection and use** of personal information must be expressly stated, and be subject to **individuals' consent**
- e) Collection of personal information **unrelated to provision of services is prohibited**

16

1. Cybersecurity Law: requirements

Cybersecurity Law
– Articles 40 - 42

Personal information protection principles (cont.):

- f) Collection and processing **must not contravene any laws**, administrative regulations and agreements with individuals
- g) Personal information **must not be leaked, tampered with or damaged**
- h) Sharing** with a third party is **prohibited without consent**
- i) Technical and other necessary steps must be taken to **ensure security**
- j) Remedial action must be taken promptly** in case of data breaches; individuals and authorities must be **notified** in a timely manner

1. Cybersecurity Law: requirements

Cybersecurity Law
– Article 43

Rights granted to individuals (as data subjects):

- a) **Right to require network operators to erase personal information** (if the network operators breach the laws or agreements with individuals)
- b) **Right to require network operators to rectify errors**

1. Cybersecurity Law: requirements

Mandatory Breach Notification to regulator and affected individuals
[Article 42]

Data localisation requirements for personal information and important data collected by operators of “**critical information infrastructure**” (CII)
[Articles 31 and 37]

- “CII”: e.g. **financial, energy, telecom and information services, water, transportation, public services, e-government** and other key industries;
- **Security assessment** is needed if there is a real necessity to transfer out of mainland China for business purposes

2. Administrative Measures for Data Security (Consultation Draft)



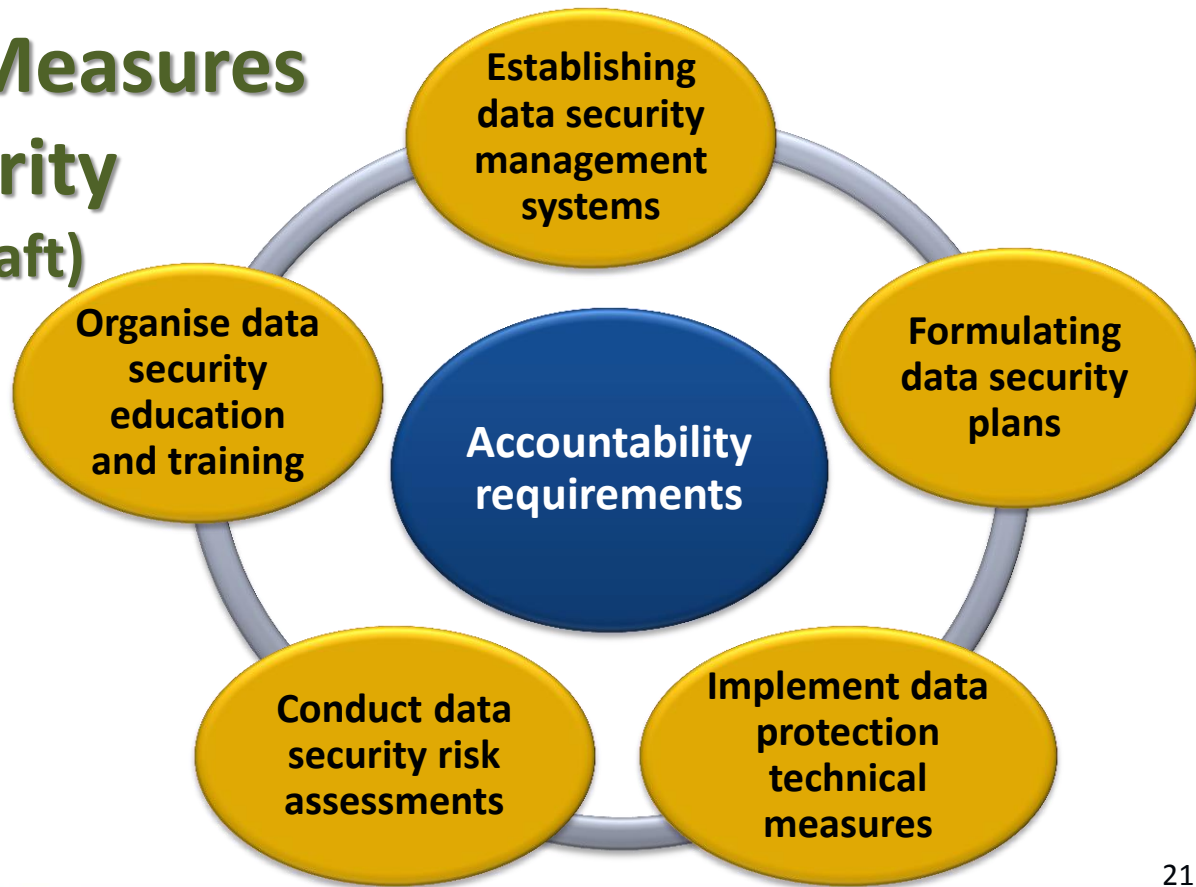
- Issued by the **Cyberspace Administration of China** on **28 May 2019**
- **Legally binding** when comes into force
- **Supplements** requirements under Cybersecurity Law
- Contains **detailed requirements** on collection, storage, transmission, processing and use of data with the aid of networks within mainland China
- Requires **registration with local chapter of cyberspace administration** for collection of **sensitive personal information** **[Article 15]**
- Allows individuals to **opt out from personalised “push notifications”** **[Article 23]**

20

2. Administrative Measures for Data Security (Consultation Draft)



Measures for Data Security Management
– Articles 6, 19



3. Measures for Security Assessment for Cross-border Transfer of Personal Information (Consultation Draft)

Issued by the **Cyberspace Administration of China** on 13 June 2019

Extends the requirements on security assessment to all network operators (vs. CII operators under Cybersecurity Law)

Legally binding when comes into force

Results of security assessment and data transfer contract be **submitted to the provincial cyberspace administration for approval [Article 3 -5]**

Provides for **requirements on security assessment** under Cybersecurity Law article 37

Extra-territoriality: applies to overseas network operators collecting personal information from China via Internet or other means **[Article 20]**

22

4. Provisions on Cyber Protection of Children's Personal Information

Came into force on 1 Oct 2019

Legally binding

Articles
1, 29

Define "children" as minors under the age of 14

Article 2

Obligations of network operators:

- Must establish specific rules and user agreements for protection of children's information
- Appoint an officer for protecting children's personal information
- Restrict access to children's personal information by staff

Articles
8, 15

Parental consent for collection, use, transfer and disclosure of children's information

Articles 9

Children and their guardians have the right to request correction and erasure

Articles
19, 20

5. Personal Information Security Specification

- ★ **Non-binding national standard** on personal information protection
- ★ 1st Edition came into force on **1 May 2018**; currently under revamp
- ★ **Most detailed guidance so far**, and similar to EU's GDPR in many aspects, e.g. (based on 2nd Edition – Consultation Draft):
 - ❖ **Wider definition of “personal information”**, including information that “*provides indications of the activities of a specific natural person*” [\[para. 3.1\]](#);
 - ❖ Requirement to appoint **data protection officer** [\[para. 10.1\]](#);
 - ❖ Data subjects’ **right to request review of automated decisions** [\[para. 7.7\]](#).
- ★ **Non-compliance** with the Specification may be **considered as a breach** of relevant requirements under other laws and regulations

6. Administrative Measures for Disclosure of Cybersecurity Threats (Consultation Draft)

Issued by **Cyberspace Administration of China** for public consultation on 20 Nov 2019

Objectives

- To prevent **illegal exploitation** of cybersecurity threats
- To **prevent profiteering** by exaggerating some cybersecurity threats for marketing purposes

Requirements

(non-exhaustive)

- **Notify relevant government authorities** before public disclosure of cybersecurity threats or security breaches
- **Must not publish certain details** about cybersecurity threats (e.g. source codes of malwares, detailed procedures of cyberattacks)

6. Administrative Measures for Disclosure of Cybersecurity Threats (Consultation Draft)

Experts' views:



Supportive: the proposed rules could help to check malicious hackers and simplify the process of reporting threats



Against: the proposed rules could limit sharing of knowledge among specialists and impair their ability to fix these security flaws

Other sectoral regulations and guidelines (non-exhaustive)

Guidelines for Data Management of
Banking Financial Institutions

Provisions on Administration of Mobile
Internet Applications Information Services

Basic Specification for Collecting Personal
Information in Mobile Internet Applications
(Draft)

Sanctions



For breaching the Cybersecurity Law and related regulations

- i. Orders for correction**
- ii. Warnings**
- iii. Confiscation of unlawful income and fining the company (max. 10 times of unlawful income or RMB 1,000,000)**
- iv. Fining responsible supervisors and other responsible personnel (max. RMB100,000)**
- v. Temporary suspension of business**
- vi. Closure of business to make correction**
- vii. Shutdown of website**
- viii. Revocation of business permits or licences**
- ix. Criminal sanctions in case of an offence**

Enforcement

[Jan 2018] MIIT summoned 3 leading tech companies due to improper practice by their apps, breaching **Cybersecurity Law**, such as:

- ambiguous privacy policies;
- insufficient disclosure on use of personal information; and
- invalid consent.

Result:

- **Ordered to rectify improper practice**

Source:http://www.xinhuanet.com/fortune/2018-01/12/c_1122251072.htm

[Apr 2018] A company in Henan was found breaching **Cybersecurity Law** by:

- collecting personal information without consent;
- excessive retention of personal information;
- not adopting adequate technical data security measures, etc.

Result:

- **Company fined RMB 50,000**
- **Directly responsible staff fined RMB 10,000**


Source:

<https://new.qq.com/cmsn/20180920/20180920011272.html>

Overview of regulations on personal information protection in mainland China:

	Collection	Use and disclosure	Transparency	Security	Retention	Accountability	Breach notification	Cross-border data transfer	Profiling and automated decision	Data access and correction	Data erasure
Cybersecurity Law	Article 41	Articles 41 & 42	Article 41	Articles 40 & 42		Article 40	Article 42	Article 37		Article 43	Article 43
Law on the Protection of Consumer Rights and Interests	Article 29	Article 29	Article 29	Article 29							
E-Commerce Law				Articles 30 & 31	Article 24		Article 30		Article 18	Articles 24 & 53	Article 24
Measures for Data Security Management (Consultation Draft) (May 2019)	Articles 11-13	Articles 22 & 27	Articles 7-9	Article 19	Article 20	Articles 17 & 18	Article 35	Article 28	Article 23	Article 21	Article 21
Provisions on Cyber Protection of Children's Personal Information	Articles 7, 9 & 11	Articles 7, 9 & 14	Articles 8 & 10	Articles 13 & 15	Articles 12 & 23	Article 8	Article 21			Article 19	Article 20
Measures for the Security Assessment for Cross-border Transfer of Personal Information (Consultation Draft) (June 2019)							Article 9	Most of the provisions			
Personal Information Security Specification (2 nd Ed. - Consultation Draft) (October 2019)	Para. 5.1-5.4	Para. 7.3	Para. 5.5	Para. 7.1, 7.2 & 10.5	Para. 6.1, 6.2, 6.4 & 7.12	Para. 10	Para. 9.1 & 9.2	Para. 8.8	Para. 7.5 & 7.7	Para. 7.8 & 7.9	Para. 7.10 & 7.12

  Legally binding (red boxes indicate more detailed requirements on data protection)

 Good practices – not legally binding

Civil protection on privacy right and personal information

1) General Provisions of the Civil Law

- ❖ In force since **July 2017**
- ❖ Recognises **privacy rights** [\[Article 110\]](#)
- ❖ Recognises that personal information of citizens is subject to **legal protection** [\[Article 111\]](#)
- ❖ Available remedies:
 - ❖ **Cease of violation**
 - ❖ **Compensation for loss suffered**
 - ❖ **Rectification of adverse effects**
 - ❖ **Restoring reputation of the affected individuals**
 - ❖ **Making apologies**

Civil protection on privacy right and personal information

2) Civil Code: Personality Rights (Draft)

- Released for consultation in August 2019
- Defines “privacy” as including **private space, private activities, private information**, etc. enjoyed by natural persons [\[Article 811\]](#)
- Outlines a number of **principles concerning the collection and processing of personal information** [\[Article 814 – 817\]](#)

Stepping up enforcement by mainland authorities

China Consumers' Association

1. Publish **inspection report** on privacy practices of 100 mobile apps in Nov 2018

2. **Urged app developers** to improve privacy practice

CAC

Ministry of Public Security

MIIT

State Administration for Market Regulation

3. Joined forces to **combat unlawful collection and use of personal information by mobile apps** in the period between January and December 2019

National Computer Virus Response Centre

4. **Named a number of popular mobile apps** for excessive collection and misuse of personal data in Sep 2019

5. Would **step up inspection** of mobile apps

Public security authorities

6. Cracked down **more than 45,000 cybercrime cases** and arrested over **60,000 suspects** in the first 10 months of 2019

Comprehensive personal information protection law in China?

- Currently on the **priority list** of the legislative agenda of the National People's Congress
- A bill is expected to be submitted to the Congress by **March 2023**



Highly fragmented
data protection laws
around the world



Interoperable
data protection
laws and policy
on a global
scale

Smoother cross-
border data flow

Better protection
for personal data

PCPD's
BOOKLET
ON CHINA
DP LAWS

Facilitate

Help companies
understand China's
data protection laws

Facilitate those
working in GBA's
data economy

35

Thank you

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

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