52nd Asia Pacific Privacy Authorities Forum 2019:

Global Privacy Forum: Bridging East and West

Recent Privacy Landscape Change in China

4 December 2019, Grand Convention Centre of Cebu, Philippines

Stephen Kai-yi WONG, Barrister

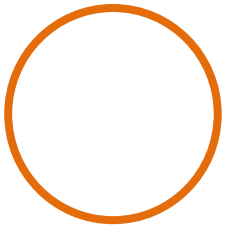
Privacy Commissioner for Personal Data, Hong Kong, China

Mainland China ’s Data Protection Regime

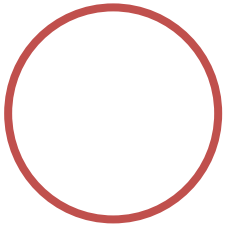
No comprehensive piece of legislation specifically directed at the protection of personal information currently

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



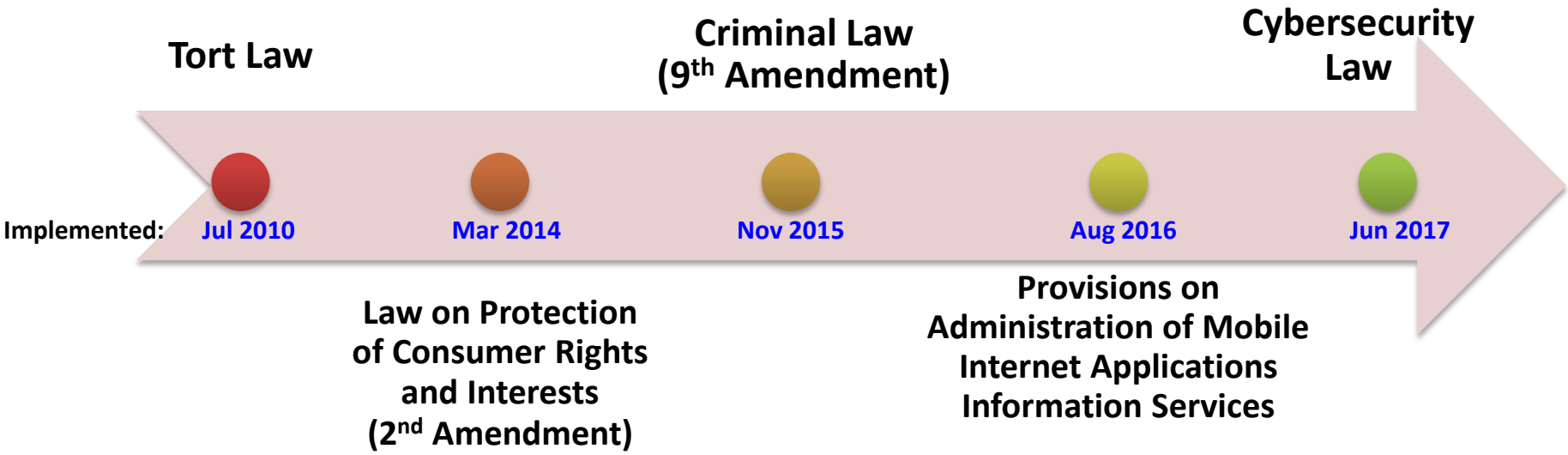
No dedicated authority with vested responsibility for enforcement of privacy and data protection laws



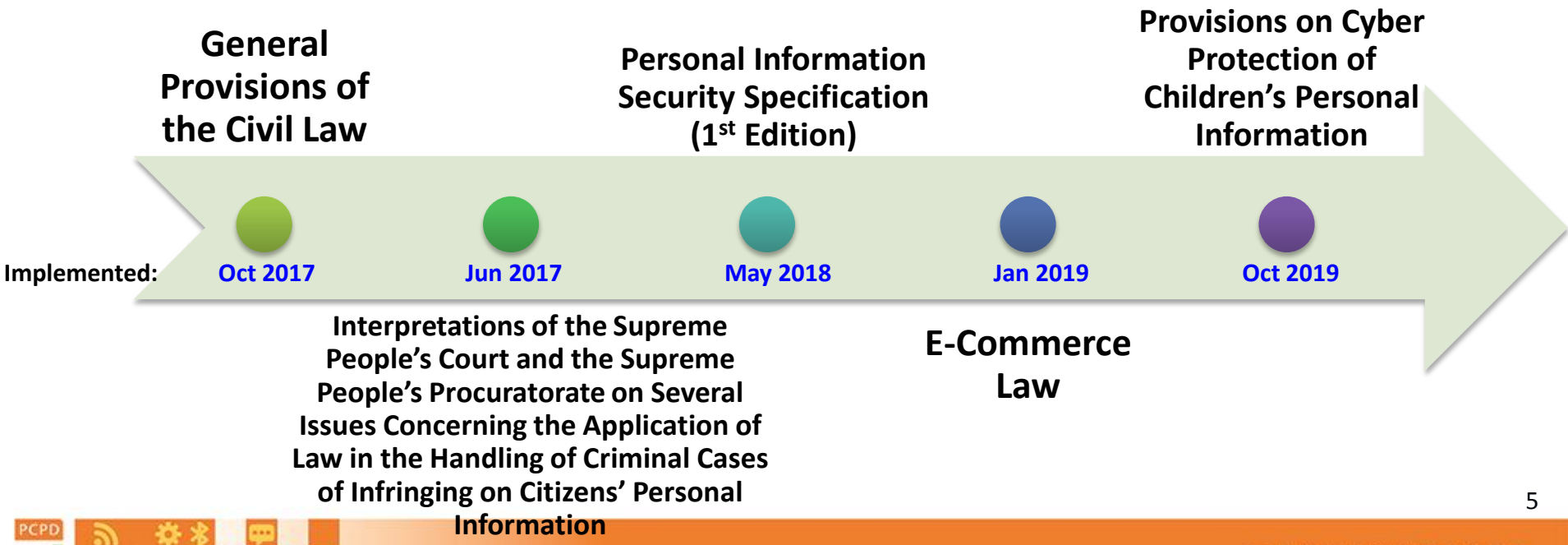
Law enforcement agencies include:

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

Laws and regulations for protecting privacy and personal information in mainland China



Laws and regulations for protecting privacy and personal information in mainland China



Other draft regulations in the pipeline

- Administrative Measures for Data Security
- Measures for the Security Assessment for Cross-border Transfer of Personal Information
- Personal Information Security Specification (2nd Edition)
- Basic Specification for Collecting Personal Information in Mobile Internet Applications
- Civil Code: Part on Personality Right

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

Regulate "Business Operators"

2nd amendment (2013) incorporated provisions for protection of personal information of consumers

- Contains high-level principles for collection, use, transparency and security of personal information [Article 29]
- Personal information protection principles similar to Cybersecurity Law

2. 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.

2. 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) the **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**;

2. 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 contractual agreements;

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.

2. 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**.

2. 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

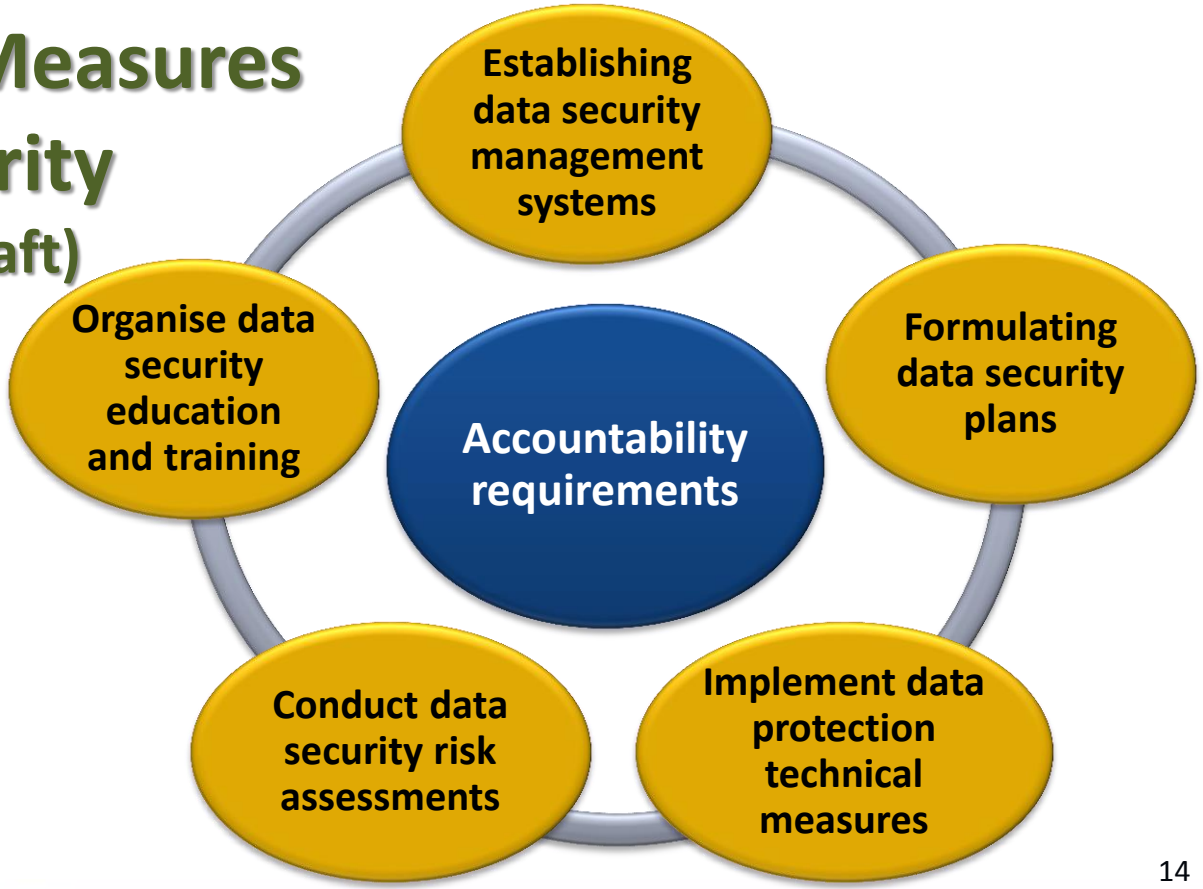
3. Administrative Measures for Data Security
(Consultation Draft)

- 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, process 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]

3. Administrative Measures for Data Security

(Consultation Draft)

Measures for Data Security Management – Articles 6, 19



4. 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

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]**

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)

Overview of requirements under various regulations 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							
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
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 (2nd 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

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)
vii. **Temporary suspension of business**
viii. **Closure of business to make correction**
ix. **Shutdown of website**
x. **Revocation of business permits or licences**
xi. **Criminal sanctions in case of an offence**

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
Chinese 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**

Thank you

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