China’s law on international movement of data and data localization in comparative an international context

Dr Brett G Williams

Principal

Williams Trade Law

Associate, Centre for Asian and Pacific Law, & Sydney Centre for International Law, University of Sydney Law School

Various domestic policy concerns affecting the field of government behaviour concerning international movement of data and local storage of data

- Issues of censorship over material available online
- Privacy of personal information
- Consumer protection
- Protecting public order
- Protecting public morals
- Protection of data from accidental loss
- Protection of data from cyber crime
- Governance of internet
- Protection of telecommunications networks
- Protecting domestic security
- Protecting intellectual property from infringement
- Protection of information disclosed to government

Measures for those purposes may Manifest as

- Restrictions on international movement of data; or
- Requirements for local storage of data

- Which can be in tension with the objectives of achieving economic benefits from :
  - Facilitating electronic transactions for international sale of goods;
  - Facilitating electronic transactions for supply of services
  - Facilitating transnational and multinational businesses choosing their optimal methods of collecting, processing and storing of data.

20th Century

- 1998 WTO Work Programme on Electronic Commerce
- - to examine trade-related issues related to global electronic commerce

Early 21st Century

- US emphasis on free movement of data:
- Reflected in FTAs containing chapters on e-commerce

- EU emphasis on data protection and protection of privacy

- EU had concerns that US government could force disclosure of data to the US government
- In 2000, US and EU agreed on EU-US Safe Harbour Rules allowing for transfer of personal data from the EU to the US (Over several year, this was replaced by revised version of similar mechanism)

Trans Pacific Partnership Agreement signed by 12 parties on 4 February 2016

- Article 14.11(2) Each party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.
- Article 14.13(2) No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.
- Both have identical exception for inconsistent measures "to achieve a legitimate public policy objective, provided that the measure:
- (a) Is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
- (b) Does not impose restrictions on the use or location or computing facilities greater than are required to achieve the objective.

- On the US announced it was not going to ratify the TPP.

EU before the 2016 General Data Protection Regulation

- 1980 OECD “Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data; 7 principles
- 1981 European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
- 1995 EU Data Protection Directive, 95/46/EC
- Superseded by
- 2016 EU General Data Protection Regulation (Regulation (EU) /679), adopted by European Parliament and Council of the EU on 14 April 2016, in force 25 May 2020

2016 EU General Data Protection Regulation

- Allows cross border transfer of data to non-EU countries only if they provide an “adequate level of protection”
- Means that protection of data is comparable to protection under the GDPR
- European Commission evaluates the receiving countries laws and practices and assesses:
  - Whether the recipient country’s privacy law provides protections comparable to protection of privacy under EU Laws; and
  - Whether the recipient country’s laws on surveillance by public authorities places sufficient limitations on their ability to access personal data, so that surveillance does not under mine privacy rights
- If a country does not have an adequate level of protection, cross border transfer of data can still be permitted if:
  - Data exporters (in EU) and data importers (outside the EU) enter into pre-approved Standard Contractual Clauses (‘SCCs); or
  - For transfers of data within a multinational company, the company has adopted Binding Corporate Rules (BCRs)

2017 Some WTO Members commence exploratory discussions on E-Commerce

- 2017 Australia, Japan and Singapore sponsored Joint Statement Initiative on E-Commerce exploratory discussions
- Not an instrument adopted by the WTO
- But 71 WTO Members jointly issued the Statement
- China did not participate
- The Statement indicated an intention to commence exploratory discussions on e-commerce.

2018 Comprehensive and Progressive Trans Pacific Partnership, ('CPTPP') concluded 23 March 2018, signed 8 January 2018,

- 11 of the 12 parties to TPP, all except the USA
- Chapter 14 on Electronic Commerce is adopted without alteration into the text of the CPTPP
- So Article 14 rules apply in relation to service providers and investors not excluded in the negative list schedules
- With prohibitions on local storage rules (14.13)
- And prohibitions on restrictions on transboundary movement of data (14.11)
- Subject to the same exceptions for legitimate policy objectives
- Article 14.8 obliges parties to maintain a legal framework for protecting personal information of users of electronic commerce.

Tracing development of Cyber law in China

- **2017 Cyber Security Law (in force 1 June 2021)**
- Introduced a framework of laws for e-commerce, including:
- **On Data Localization:**
- Section 37 requires data collected or produced in China to be stored in China;
- **On international movement of data:**
- **Section 37** provides that persons wishing to transfer data outside of China must obtain a security clearance under measures formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council
- **Penalties under section 66** – suspension of business, loss of business licence, shut down of website, fines
- Rules apply to what critical information operators do with network data

2019 WTO Joint Statement Initiative negotiations commence

- 91 Members commence negotiations with a view to creating an agreement on E-Commerce
- China is part of the group
- USA was leading proposer for the text to include:
  - A prohibition on data localization laws (Law requiring that data collected in a country had to be stored in that country); and
  - General freedom of movement of data across transnational borders; A prohibition on laws restricting international movement of data.

1 Jan 2020, *US-Mexico-Canada Agreement* ('USMCA') in force

- Same clause as in TPP

- Article 19.11(1) No party shall prohibit or restrict the cross-borer transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.
- With an exception to 19.11(1) for legitimate public policy objectives
- Article 19.12 No party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.
- There is a NO legitimate public policy objective exception to Article 19.12.

Digital Economy Partnership Agreement between Chile, New Zealand and Singapore, signed 12 June 2020, in force 28 December 2020,

- Contains their existing obligations under CPTPP
- Art 4.3(2) is a commitment to allow data to move freely across borders “when this activity is for the conduct of the business of a covered person”
- Article 4.4(2) prohibits data rules requiring covered person to use or locate computing facilities in that territory “as a condition of doing business in that territory.”
- Both have an exception for inconsistent measures to achieve a legitimate public policy objective, provided that the measure:
- Is not applied in a manner which would constitute an arbitrary or unjustifiable discrimination or a disguised restriction on international trade; and
- Does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

- Korea has acceded, China has applied to accede.

Signed 15 Nov 2020, *Regional & Comprehensive Economic Partnership Agreement* (‘*RCEP*’) in force for 10 parties 1 Jan 2022

- The 7 Asian parties to CPTPP + Cambodia, China, Indonesia and South Korea
- Art 12.14(2) and 12.15(2) Same two obligations but exceptions are wider
- Nothing in this Article shall prevent a Party from adopting or maintaining:
- (a) any measure inconsistent with para 2 **that it considers necessary to achieve** a legitimate public policy objective provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or
- (b) Any measure **that it considers necessary** for the protection of its essential security interests. Such measures shall not be disputed by other Parties.

Further development of cyber law in China:

- *Data Security Law*, adopted by NPC June 2021, in force 1 Sept 2021

- *Personal Information Protection Law*, adopted by NPC 20 August 2021, in force 1 Nov 2021.

- A series of implementing regulations issued by Cyberspace Administration of China, setting out more details of the application of the rules in the DSL and PIPL , including:
- *Measures for Security Assessment of Outbound Data Transfer* 2022
- *Measures on Standard Contracts for Outbound Transfers of Personal Information* 2023
- *Announcement on the Implementation of Personal Information Protection Certification* 2022

Data Security Law, adopted June 021, in force Sept 2021

- applies to all processing of any data by any data processor(see Definitions in article 3) (whereas *Cyber Security Law* 2016 applied only to 'critical information operators' and to 'network data')
- Covers collection, storage, processing, transmission of all information collected in electronic form
- Art 6 Allocates responsibilities to Ministries and overall planning responsibility to national Cyberspace affairs department
- Art 8 obliges all data processors to fulfill data protection obligations, and not endanger national security and public interests, nor harm lawful rights and interests of individuals
- Article 21 "The State shall establish a categorized and classified system and shall carry out data protection based on the importance of the data in economic and social development, as well as the extent of harm to national security, public interests, … interest of individuals [if the data is] … illegally obtained or used.

Data Security Law, adopted June 2021, in force Sept 2021 , continued

- Article 30 oblige data processors to conduct risk assessments of their data processing, on a regular basis and to file risk assessment reports with relevant departments.
- Article 31
- Provisions of *Cyber Security Law* on outbound security management (prohibiting transboundary movement of data without a security clearance) apply to important data collected by information infrastructure operators in China
- And measures for outbound security management of important data collected or produced by other data processors in China shall be formulated by the national cyberspace authorities.
- Article 46 provides for penalties for breach of Article 31, fines, loss of business license
- Meaning of ‘information infrastructure operators’ defined in a subsequent regulation
- Meaning of ‘important data’ defined in a subsequent regulation

Personal Information Protection Law, adopted by NPC 20 August 2021, in force 1 Nov 2021.

- China's first comprehensive privacy law

Includes provisions on:

Art 6 collection of personal information shall be limited to the minimum scope required for the purpose of processing

Art 7 rules for processing personal information shall be disclosed

Art 9 Personal information processors must take measures to ensure the security of the personal information they process

Art 19 that the storage time should be the minimum time necessary to achieve the purpose of processing

Personal Information Protection Law, adopted by NPC 20 August 2021, in force 1 Nov 2021.

- On data localization:
- Article 40 applies to critical information infrastructure operators and to personal information processors
- Requires the personal information collected and generated in China to be stored in China
- And can only provide the information to a party outside China subject to a security assessment organized by the national cyber space department.

Personal Information Protection Law, adopted by NPC 20 August 2021, in force 1 Nov 2021.

- Article 38 Cross-border transfer of personal data outside of China is permitted only if:
- The individual has consented
- There is a legitimate and pre-defined purpose
- Transferor must ensure that the recipient country provides an adequate level of protection
- ‘adequate level of protection’ I focussed on protection of national security (in contrast to the EU adequate level of protection which is focussed on protection of privacy)
- If the destination country does not provide an adequate level of protection, then:
- The data exporter must conduct a security assessment and the Chinese authorities may require additional security reviews; and
- Either
- The data exporters and the data importer enter into Standard Contractual Clauses (SCCs) containing obligations of parties to ensure that the data is protected to the same standard as is required within China.

WTO JSI stabilized text

- 2023 USA withdrew its proposals on freedom of movement of data, and on prohibiting data localization

- 2024 Stabilised text completed.
- The text is silent on data localization rules.
- A silent on international movement of data.

Observations, cautions

- If China's movement of data and data localization rules are too onerous or too strict with respect to national security:
- Some foreign investors will choose to establish a branch in some country other than China instead of investing in China,
- They may prevent movement of information that would be necessary to satisfy traceability of Chinese goods

Appendices: extracts from legislation and treaties

- PRC **Cyber Security Law 2017**
- Section 37 “Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People’s Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.”

Cyber Security Law 2017, section 66 provides for penalties for breach of section 37

- Where critical information operators violate Article 37 of the Law by storing network data outside the mainland territory, or provide network data to those outside of the mainland territory, the relevant competent department: shall order corrective measures, provide warning, confiscate unlawful gains, and levy fines between RMB 50,000 and 500,000; and may order a temporary suspension of operations, a suspension of business for corrective measures, closing down of websites, revocation of relevant operations permits or cancellation of business licenses. Persons who are directly in charge and other directly responsible personnel shall be fined between RMB 10,000 and 100,000.

Data Security Law of the PRC,

- Adopted at the 29th meeting of the Standing Committee of the Thirteenth National People's Congress of the PRC on June 10, 2021. In force 1 September 2021

Data Security Law, 2021, Article 31

- “The provisions of the Cyber Security Law of the People's Republic of China shall apply to the outbound security management of the important data collected or produced by critical information infrastructure operators during their operation within the territory of the People's Republic of China, and the measures for the outbound security management of the important data collected or produced by other data processors during their operation within the territory of the People's Republic of China shall be formulated by the national cyberspace authority in conjunction with the relevant departments under the State Council.”
- Article 46 provides for penalties for breach of Article 31.

Personal Information Protection Law

- Adopted at the 30th Meeting of the Standing Committee of the Thirteenth National People's Congress on August 20,2021,

- In force on 1 November 2021

PIPL, transboundary movement of data: Article 38

- A personal information processor that truly needs to provide personal information for a party outside the territory of the People's Republic of China for business sake or other reasons, shall meet one of the following requirements:
- (1) passing the security assessment organized by the national cyberspace department in accordance with Article 40 of this Law;
- (2) obtaining personal information protection certification from the relevant specialized institution according to the provisions issued by the national cyberspace department;
- (3) concluding a contract stipulating both parties' rights and obligations with the overseas recipient in accordance with the standard contract formulated by the national cyberspace department; and
- (4) meeting other conditions set forth by laws and administrative regulations and by the national cyberspace department.

PIPL, 2021, transboundary movement of data, Article 38 continued

- Where an international treaty or agreement that the People's Republic of China has concluded or acceded to stipulates conditions for providing personal information for a party outside the territory of the People's Republic of China, such stipulations may be followed.
- The personal information processor shall take necessary measures to ensure that the personal information processing activities of the overseas recipient meet the personal information protection standards set forth in this Law.

[from website of National People’s Congress

Personal Information Protection Law of the People's Republic of China

PIPL, 2021, data localization

- Article 40 Critical information infrastructure operators and personal information processors whose processing of personal information reaches the number prescribed by the State cyberspace administration shall store the personal information collected and generated within the territory of the PRC within the territory of China. If it is indeed necessary to provide such information and data to overseas parties, it shall be subject to the security assessment organized by the State cyber space administration; if laws, administrative regulations or the provisions of the State cyberspace administration provide that the security assessment is not required, such provisions shall prevail.