SANTA CLARA UNIVERSITY
SCHOOL OF LAW

Chinese Privacy Law

and Its Impact on Foreign Businesses in China

Anna M. Han, Professor of Law, Santa Clara Law
Yuanyuan (Yvonne) Cheng, Partner, King & Wood Mallesons
Jason Chang, Of Counsel, DLA Piper

November 16, 2021

SANTA CLARA LAW

Anna M. Han
Professor of Law
Santa Clara Law

ahan@scu.edu

Personal Information Protection Law (PIPL)

SANTA CLARA LAW

China's Personal Information Protection Law ("PIPL") was finalized on August 20, 2021, and became effective on November 1, 2021.

PIPL Highlights

SANTA CLARA LAW

1. General

PIPL and the Cybersecurity Law and Data Security Law should be taken as a package for privacy professionals and provides a framework for analysis.

China's notion of privacy is different - it applies to private actors, not the government. The amount of monitoring and personal information collected by the government is voluminous.

PIPL Highlights

SANTA CLARA LAW

2. Scope

PIPL applies to organizations

- **handling personal information of natural persons inside China, and**
- **handling personal information of natural persons inside China even if the organization is outside of China if:**
  a. **Purpose is to provide goods/services to persons in China**
  b. **Analyzing or assessing activities of persons in China**
  c. **Other circumstances provided in laws or administrative regulations**

PIPL Highlights

SANTA CLARA LAW

3. What is “Personal Information”?

“Personal information” means any kind of information relating to an identified or identifiable natural person, either electronically or otherwise recorded, but excluding information that has been anonymized.

PIPL Highlights

SANTA CLARA LAW

4. What is “Sensitive Personal Information”?

Sensitive personal information refers to the personal information that can easily lead to the infringement of the personal dignity or natural persons or the harm of personal or property safety once leaked or illegally used, including such information as biometrics, religious belief, specific identities, medical health, financial accounts, and whereabouts, and the personal information of minors under the age of 14.

PIPL Highlights

SANTA CLARA LAW

4. Consent and Other Legal Basis For Obtaining Information:

a) **Consent**
b) **Necessity for contracts or human resources (HR) management**
c) **Statutory duties or statutory obligations**
d) **Protection of the life, health, and property safety**
e) **Public interest**
f) **Personal information already disclosed**

PIPL Highlights

SANTA CLARA LAW

5. Consent

Consent is only valid if individuals voluntarily and explicitly provide such consent and with full knowledge of the details of the personal information processing. Art. 14-15.

Individuals also have a right to withdraw consent, and personal information processors must provide individuals with a convenient means of withdrawing consent.

PIPL Highlights

SANTA CLARA LAW

6. Extraterritorial Effect

The PIPL has extraterritorial effect and will apply to overseas entities that do not have a presence in China but that process personal information of natural persons located in China for(1) offering goods or services to them in China, or (2) analyzing and evaluating their behavior, or (3) under other circumstances specified by laws or administrative regulations.

PIPL Highlights

SANTA CLARA LAW

7. Cross-Border Transfer of Personal Information

Like the the GDPR, the PIPL places restrictions when it comes to cross-border data transfers but adds additional approval.

SANTA CLARA LAW

7.1 Separate, explicit consent must be obtained for the following activities - open issue awaiting further regulation

(a) processing sensitive personal information;
(b) overseas transfers;
(c) public disclosure of personal information;
(d) to provide data to another data controller for processing; and
(e) use of image or identification data collected in public through image or identification device for any purposes other than maintaining public security. (This aligns with other recent guidance putting clearer parameters around use of biometric data in China).

SANTA CLARA LAW

7.2 Overseas Transfers/Data Localization

(a) **Data controllers may only transfer or access personal information outside of Mainland China under specific circumstances (PIPL Art. 38-39).**

(b) **However, certain personal information (and non-personal data) must still remain in (and cannot be accessed outside of) Mainland China (PIPL Art. 40).**

SANTA CLARA LAW

7.3 Foreign Government Access to/Disclosure of Personal Information

(a) Data controllers must not provide personal information stored within China to overseas legal or enforcement authorities unless approval is obtained from a designated Chinese authority.

(b) Chinese authorities may provide personal information stored within China to overseas legal or enforcement authorities upon request, if and to the extent that there are international treaties or regulations in place to maintain fairness and for mutual benefit.

SANTA CLARA LAW

8. Penalty

Serious violation of the PIP Law could lead to a fine up to RMB 50 million (about USD 7.76 million) or 5% of the company's annual revenue for the prior year.

SANTA CLARA LAW

9. Article 58 Additional Obligations for IIPPs; Large Volume Controllers; and/or Complex Businesses

Organizations that fall into one of the following categories (not yet defined):

(a) "important internet platform providers";
(b) data controllers processing data of a "large volume of users"; or
(c) "complex businesses", must comply with additional measures when processing personal information

Are subject to additional requirements: (i) establish an independent organization to supervise processing activities; (ii) follow the principles of openness, fairness and justice; (iii) immediately cease their service offerings when in serious violation of the law; and (iv) regularly publish reports on social responsibility of PI handling

Open Issues

SANTA CLARA LAW

1. Separate, explicit consent must be obtained for the following activities.

(a) It remains unclear what "separate" consent means in practice. For now, it appears to suggest organizations should avoid bundled or forced consent to such activities, especially on app interfaces.

2. "important internet platform providers"remain undefined.

3. The volume of data processed by "large volume of users" remains undefined.

2 Key Highlights

SANTA CLARA LAW

1. The PIPL applies to all data handling activities involving personal information within China, and also applies to activities outside China that affect individuals within China. In particular, the PIPL imposes extensive notice and consent requirements on companies that wish to handle personal information, and also imposes significant hurdles for companies that wish to engage in the cross-border transfer of personal information.

2. Implementing regulations and further guidance concerning the PIPL are expected in due course, but in view of the November 1 effective date of the PIPL, companies should immediately start reviewing and assessing their data processing activities against the PIPL's requirements.

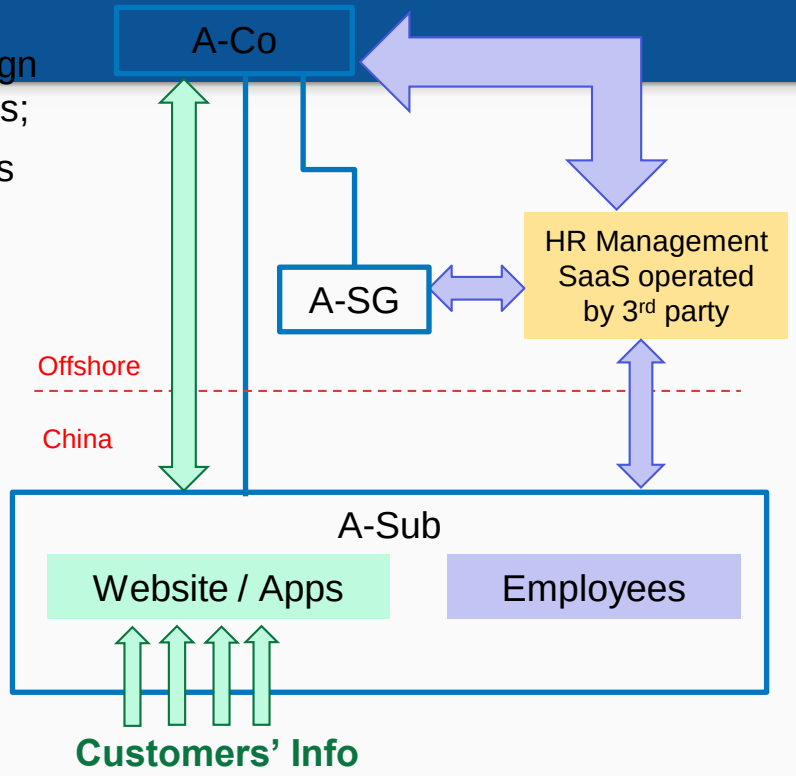
SANTA CLARA LAW

Yuanyuan (Yvonne) Cheng
Partner, Silicon Valley & Beijing Office
King & Wood Mallesons

chengyuanyuan@cn.kwm.com

Case Study (I)

- A-Co is a U.S. based online design company, which offers its website and App for users to do graphic design by using its online tools, templates and other resources;
- A-Co has a subsidiary in China (A-Sub) which provides the same services to Chinese customers via the Chinese website and mobile Apps; Chinese customers' data will be sent back to the U.S. for personas;
- A-Sub has about 10 employees in China. Due to the limited size of the company, A-Sub's HR affairs are in general managed by A-Co's Singapore office (A-SG) through an HR management solution provided by a third party as SaaS (with the main server located outside of China) and China employees' information will be uploaded to such SaaS server, and then be accessible by HR managers in both A-SG and A-Co.



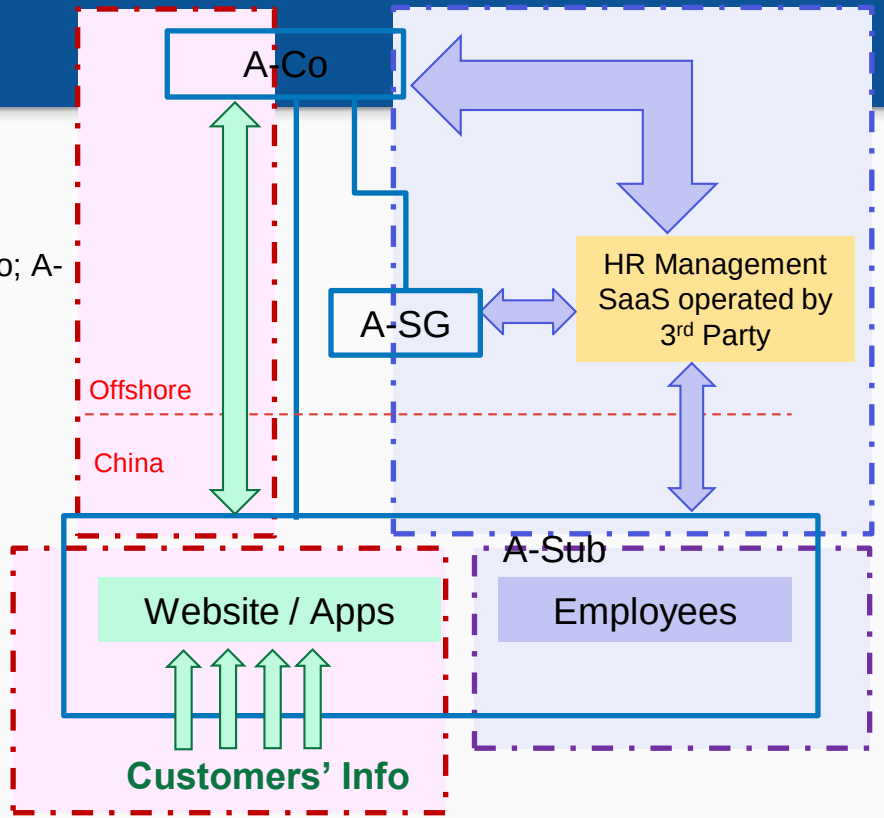
Case Study (I)

SANTA CLARA LAW

- Customers' PII:
  Within China:
  - ✓ Privacy policies; cookies policies;
  - ✓ Compliance re PII processing;

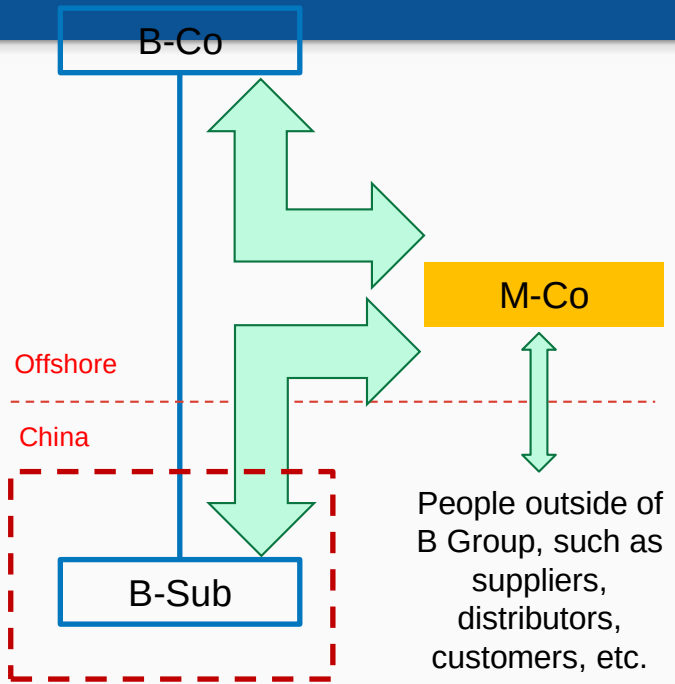
  Outside of China:
  - ✓ Cross-border transfer of PII;
  - ✓ Data processing agreement between A-Sub and A-Co; A-Co's compliance as a foreign PII processor.
- Employees' PII
  Within China:
  - ✓ Employment Contract; Employee Handbook
  - ✓ Compliance re PII processing;

  Outside of China
  - ✓ Cross-border transfer of PII; data sharing with other PII processor(s)
  - ✓ Data processing agreement between A-Sub and A-Co/A-SG;
  - ✓ Data processing agreement between A-Sub and third-party.



Case Study (II)

- B-Co is a U.S. based MNC, which manufactures and sells cosmetics products around the world.
- B-Co has a subsidiary in China (B-Sub) which sells B-Co's products in China. In general, B-Sub processes PII (including employee data, suppliers' data, distributors' data and customers' data) locally.
- B-Co uses M-Co as an email service provider globally. All of B Group's emails (including B-Sub's emails), in and out, even internal emails between two Chinese employees of B-Sub, will first go through M-Co's servers in Japan and several other jurisdictions, where the servers will filter suspected spam and virus and then deliver the emails to the relevant addressees.

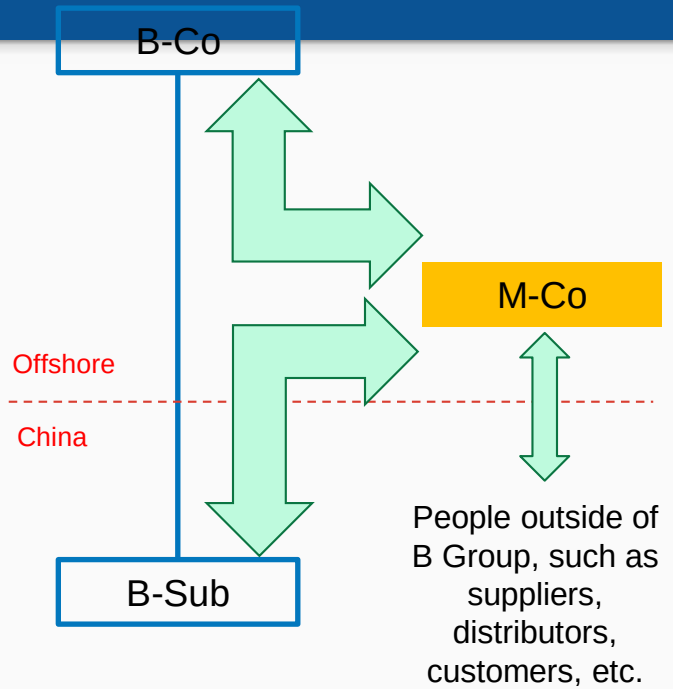


Case Study (II)

SANTA CLARA LAW

- Inform the suppliers and customers about the cross-border data transfer associated with the email services? Obtain a "separate consent" from the relevant suppliers and customers regarding cross-border PII transfer? What if the email conversation involves PII of a third party who is neither the sender or the addressee?

  For example: An employee of a Chinese distributor sends an email to an employee of B-Sub in China, reporting a Chinese customer's complaint about allergies, with the consumer's name, phone number, shopping records, photos showing the allergies, medical records about the allergies … Cross-border PII transfer occurs when the email is sent, without the customer's awareness and consent.

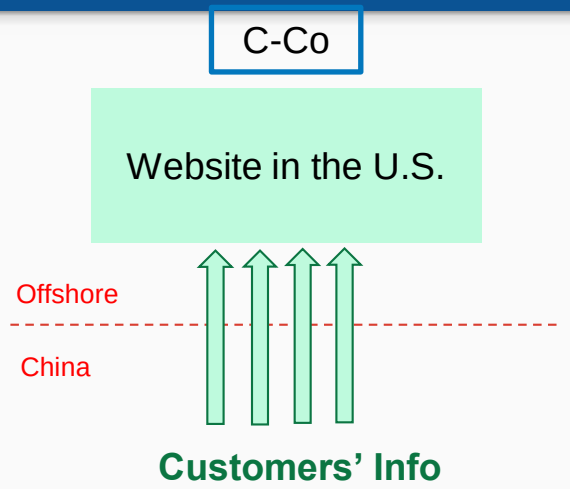


Case Study (III)

- C-Co is a U.S. based fashion company, which produces and sells jewelries and cloths.

- Chinese customers visit C-Co's offline stores when they travel to the U.S. and they may provide C-Co with their PII (such as name, phone number or mailing address, favor) if they choose to register as a "member"; and C-Co may send them brochures and small gifts from time to time.

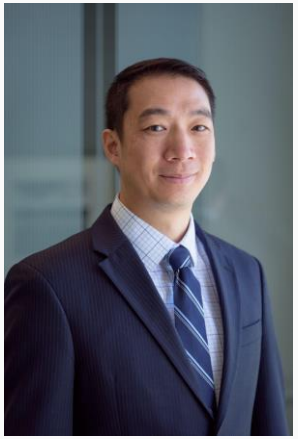
- In addition to offline stores, C-Co also sells its products via its company website, the server of which is located in the U.S. From time to time, there are customers located in China (identified based on the delivery address) visiting C-Co's website and purchasing stuffs. For the purpose of the transactions, the customers from China would need to provide their credit card information (or Paypal information) and name and address for delivery.



Case Study (IV)

- D-Co is a U.S. company and it has a subsidiary in China (“D-Sub”).
  - D-Co conducts an internal FCPA investigation, and requests D-Sub to provide the U.S. head office with all of the email communication of D-Sub in the past several years;
  - D-Co is under FCPA investigation by the US government and is requested to provide all records of the D-Sub executives

SANTA CLARA LAW



Jason Chang
Of Counsel, DLA Piper

jason.chang@dlapiper.com

PRC Data Compliance for Litigation and Investigations

SANTA CLARA LAW

How do these laws impact US litigation and/or investigation?

- SEC/DOJ investigation
- Subpoena, discovery, document/information request
- Deposition, witness interview
- Corporate / internal investigation
- US litigation / arbitration
- Document preservation / collection

What's New? Article 41 of the PIPL and Article 36 of the DSL both require an approval of the Chinese competent authorities when dealing with data requests from foreign judicial or law enforcement agencies for personal information or data stored within China.

PRC Data Compliance for Litigation and Investigations

SANTA CLARA LAW

Threshold Questions

1. Where is the data located? (PRC mainland or overseas?)
2. Did the data originate from China?
3. Are there PRC nationals involved?

Map Out Your Data

1. Types of data involved (Emails, servers, laptops, mobile devices, etc.)
2. Company-issued device or BYOD?
3. Company's policies and procedures?
4. Employment agreement, PRC handbook, etc.

Substantive Considerations

- Personal information
- Important / sensitive information
- State secrets / PRC national security related issues
- Audit work papers
- Confidentiality between parties
- Large pools of personal information (e.g. databases, excel spreadsheets)
- Data from the government/government officials

PRC Data Compliance for Litigation and Investigations

SANTA CLARA LAW

Reviewing and Producing Documents

- Substantive review conducted within mainland China
- Clear documents prior to export and production
- Obtain separate consent
- Redaction of documents where required (e.g. personal information)
- PRC law firm memo and/or log of documents redacted/withheld where required