TechCrunch

September 9, 2021

Extra Crunch

What China's new data privacy law means for US tech firms

Scott W. Pink Contributor
Scott Pink@omelvenymyers

China enacted a sweeping new data privacy law on August 20 that will dramatically impact how tech companies can operate in the country. Officially called the Personal Information Protection Law of the People's Republic of China (PIPL), the law is the first national data privacy statute passed in China.

Modeled after the European Union's General Data Protection Regulation, the PIPL imposes protections and restrictions on data collection and transfer that companies both inside and outside of China will need to address. It is particularly focused on apps using personal information to target consumers or offer them different prices on products and services, and preventing the transfer of personal information to other countries with fewer protections for security.

The PIPL, slated to take effect on November 1, 2021, does not give companies a lot of time to prepare. Those that already follow GDPR practices, particularly if they've implemented it globally, will have an easier time complying with China's new requirements. But firms that have not implemented GDPR practices will need to consider adopting a similar approach. In addition, U.S. companies will need to consider the new restrictions on the transfer of personal information from China to the U.S.

Implementation and compliance with the PIPL is a much more significant task for companies that have not implemented GDPR principles.

Here's a deep dive into the PIPL and what it means for tech firms:

New data handling requirements

The PIPL introduces perhaps the most stringent set of requirements and protections for data privacy in the world (this includes special requirements relating to processing personal information by governmental agencies that will not be addressed here). The law broadly relates to all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, but excludes anonymized information.

The following are some of the key new requirements for handling people's personal information in China that will affect tech businesses:

Extra-territorial application of the China law

Historically, China regulations have only been applied to activities inside the country. The PIPL is similar in applying the law to personal information handling activities within Chinese borders. However, similar to GDPR, it also expands its application to the handling of personal information outside China if the following conditions are met:

- Where the purpose is to provide products or services to people inside China.
- Where analyzing or assessing activities of people inside China.
- Other circumstances provided in laws or administrative regulations.

For example, if you are a U.S.-based company selling products to consumers in China, you may be subject to the China data privacy law even if you do not have a facility or operations there.

Data handling principles

The PIPL introduces principles of transparency, purpose and data minimization: Companies can only collect personal information for a clear, reasonable and disclosed purpose, and to the smallest scope for realizing the purpose, and retain the data only for the period necessary to fulfill that purpose. Any information handler is also required to ensure the accuracy and completeness of the data it handles to avoid any negative impact on personal rights and interests.

Consent generally required

Subject to certain exceptions, consent is required to handle personal information and individuals have the right to rescind their consent. A company cannot refuse to provide products or services if an individual does not consent to the handling of their information or rescinds their consent, except where handling the data is necessary to provide products or services.

The exceptions to consent include: (a) Where necessary to conclude or fulfill a contract in which the individual is an interested party, or where necessary to conduct human resources management; (b) where necessary to fulfill statutory duties and responsibilities or statutory obligations; (c) where necessary to respond to sudden public health incidents or protect people's lives and health, or the security of their property, under emergency conditions; and (d) within a reasonable scope, to implement news reporting, public opinion supervision, and other such activities for the public interest.

The law also has a public disclosure exception in that consent is not required for handling personal information disclosed by persons themselves or otherwise already lawfully disclosed within a reasonable scope. This could apply to information posted on public websites.

Separate consent is also required to disclose information to another information handler. The transferring party must also notify the individual of the transfer, including the contact name or personal name of the recipient, their contact method, the handling purpose, handling method and information categories transferred.

Sensitive personal information

Special protections apply to sensitive personal information — information that can easily cause harm to people's dignity or grave harm to personal or property security. This includes biomet-

ric characteristics, religious beliefs, specially designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14. Companies are required to conduct data-impact assessments when handling sensitive personal information.

In general, a company cannot handle sensitive personal information unless there is a specific purpose and sufficient necessity for that information and special protection measures are put into place. The company must notify the individual of the purpose and need, and obtain their consent (and the consent of the parent or legal guardian for a child under 14). There are no exceptions for consent relating to sensitive personal information.

Notice requirements

Similar to GDPR and other data privacy laws, before handling the personal information, the data handler must notify individuals truthfully, accurately, and fully of the following items using clear and easily understood language: (a) the name or personal name and contact method of the information handler; (b) the purpose and the handling methods, the categories of handled information and the retention period; and (c) methods and procedures for individuals to exercise the rights provided in the law. Regulations will likely further define what must be included in the notice.

Individual rights

The PIPL provides a number of individual rights, including: (a) the right to know and decide relating to the use of their personal information, as well as to limit or refuse the handling of their information by others; (b) the right to consult and copy their information; (c) the right to transfer their information to another handler they designate; (d) the right to request correction or completion of their information; and (e) the right to request an explanation of their information handling.

The PIPL also introduces a requirement that information handlers must proactively delete the data once the purpose is achieved or the information is no longer needed; or if the purpose is impossible to achieve; the handler has ceased providing products and services; the retention period has expired; the individual rescinds consent, or the information has been used in violation of laws or agreements. In addition, people can also request deletion of their information.

Information handlers are required to establish convenient mechanisms to accept and handle people's requests to exercise their rights. They are also required to explain any reasons for rejecting such requests.

Perhaps most significantly, unlike many U.S. privacy laws, which have no private right of action and are only enforced by regulation, the PIPL allows an individual to file a lawsuit with a People's Court if personal information handlers reject individuals' requests to exercise their rights.

Security

The PIPL requires personal information handlers to implement data protections, including: (a) formulating internal management protocols and operating rules; (b) implementing categorized management of personal information; (c) adopting technical security measures such as encryption and de-identification; (d) determining operational limits for personal information handling, and regularly conducting security education and training for employees; and (e) formulating and organizing the implementation of personal information security incident response plans.

In particular, critical internet platform service providers that have a large number of users and operate complex types of business would need to establish an independent body mainly composed of external members to supervise their protection of personal information.

Impact on mergers and acquisitions

The PIPL will likely impact corporate transactions, such as mergers, separations, dissolutions and bankruptcies. First, the transferring party must notify individuals about the receiving party's name or personal name and contact method. The receiving party must also continue to fulfill the transferring party's duties and cannot change the purpose or method of handling personal information without notifying the individual, and where applicable, obtaining consent.

Automated decision-making

The PIPL, like the GDPR, entitles individuals to refuse automated decision-making if the decision has a significant impact on their rights and interest. It does not define which activities might be covered, although it is likely to cover such decisions as loan and credit approvals. The PIPL also does not provide any exceptions to this right of refusal. This is likely to be clarified by further regulation.

Targeting/price discrimination

One of the regulators' major concerns involved consumers claiming that internet companies were violating customer rights by misusing personal data and using price differentials in services being offered to force a consumer to use a particular product or service. For example, complaints were raised about ride-sharing apps allegedly charging consumers more for hailing a taxi using an iPhone than a cheaper mobile phone model, or for tickets if they are profiled as a business traveler.

The PIPL prohibits personal information handlers from engaging in unreasonable differential treatment of individuals in trading conditions such as trade price. App developers using push delivery or commercial sales to individuals through automated decision-making methods must provide a targeting-free option or a convenient method for individuals to refuse such targeted advertising or delivery.

Data protection officers and representatives

Handlers of large quantities of personal information that exceeds an amount threshold designated by the national cyberspace authority are required to appoint a data protection officer. Companies outside of China caught by the exterritorial jurisdiction of the PIPL must establish a dedicated agency or appoint a representative in China to handle data protection matters.

Cross-border transfers

The PIPL introduces restrictions on the transfer of personal information out of China for business or other needs. To make such a transfer, a company must:

- Pass a security assessment organized by the national cybersecurity authority.
- Undergo personal information protection certification conducted by a specialized body according to provisions established by such regulators.
- Enter a contract with the foreign receiving side in accordance with a standard contract formulated by regulators — likely to be an approach similar to the Standard Contractual Clauses adopted by the European Union.
- Or, meet other conditions provided in laws or administrative regulations or by the national cybersecurity authority.

The transferring party must ensure that the foreign receiving parties' information handling activities

reach the standard of information protection provided under the PIPL — essentially exporting the PIPL protections to the foreign entity.

In addition, the transferring party must also notify the individual about the receiver's name, contact information, handling purpose, handling methods and categories of the personal information to be transferred, as well as ways and procedures for individuals to exercise their rights with the receiver and other such matters, and obtain individuals' separate consent.

Data storage

Companies will need to consider whether they must store personal information they collect in China. The 2017 Cybersecurity Law only requires critical information infrastructure operators (CIIOs) to store collected personal information in China. The new law expands this localization requirement to personal information handlers handling large quantities of data.

The information stored by such companies cannot be transferred out of China unless the company passes a security assessment organized by the national cybersecurity authority, or unless a statutory exception (e.g., arrangement under international treaties or protocols that China acceded) applies. Without the approval of authorities, data handlers shall not provide any information stored in China to a foreign judicial or law enforcement body.

Compliance steps and challenges for U.S. companies

American firms doing business in China or with companies inside China will need to immediately start assessing how this new law will impact their activities. For example, if you operate an autonomous vehicle company trying to enter China, you will need to comply with the full range of the new law's requirements with respect to sales of the product in China, including providing notices in connection with the sales process and obtaining consent as required.

If you are providing financing for purchases, you must consider whether loan decisions involve automated decision-making, for which you will need to provide consumers an option for individualized decision-making. If you are marketing to Chinese residents, you must consider providing them an option to opt-out of targeted advertising. If you collect data from the vehicles themselves, you may have to provide special notice and obtain consent for such data collection, as it may be considered sensitive personal information.

You also may have to consider storing such data in China, particularly if it meets the thresholds set by regulators for localized storage. You may further need to conduct security assessments or obtain certifications to allow transfer of the data to the United States.

If you are a biotech or hardware device company with manufacturing and production facilities in China, your main focus will be regarding employee and contractor data. Consent is likely not required to collect much of the data since it falls under the exception for human resource management, but notice should be provided and consent is required for sensitive data. Consent may also be required if you want to disclose the information to third parties, such as payroll processors.

If a company already complies with GDPR, then the focus will be on making changes to reflect differences in the Chinese law, obtaining consents and ensuring that data can be transferred across borders. For cross-border data transfer, a company will need to determine if it is a CIIO or processor of large quantities of data that needs special governmental approval.

Implementation and compliance is a much more significant task for companies that have not implemented GDPR principles. It should involve a structured approach starting with a data inventory and mapping that examines the types of personal information collected in China and the purpose of the collection.

Based on that information, the company should start assessing the following:

- Whether consent is required and how to obtain such consent.
- Preparing notices that contain the disclosures and methods for exercise of data subject rights.
- Implementing processes for responding to data subject requests.
- Implementing processes for deletion of data after it is no longer needed or retention periods expire.
- Ensuring that it has provided notice and obtained consent for disclosures to third parties.
- Ensuring that third parties agree to comply with the security and privacy requirements of the PIPL.
- Determining whether localized data storage may be required and implementing processes (such as using certifications, approved contracts or obtaining government approval) for cross-border transfers.
- Determining whether to appoint a data protection officer and identifying and appointing a data representative in China.

Starting this process early will ensure a more orderly transition and reduce the risks of any interruption in business operations in China.

Disclaimer: The views expressed here are those of the author and do not necessarily reflect the views of O'Melveny & Myers, LLP.

Scott W. Pink is special counsel in O'Melveny's Data Security & Privacy practice based in Silicon Valley. He advises technology, media, entertainment and a variety of companies on issues of cybersecurity and privacy, IP counseling; social media law; and advertising, marketing, and promotions law.