wiley

NEWSLETTER

# U.S. Businesses Must Navigate Significant Risk of Chinese Government Access to Their Data

March 2021

*Privacy In Focus*®

U.S. and other foreign businesses operating within the People's Republic of China (PRC) or doing business in the PRC should be aware of significant risks associated with the PRC government's authority to access sensitive intellectual property, proprietary commercial secrets, and personal data (of employees, users, or customers). The PRC has promulgated a number of broad and ambiguously worded laws, many of which have extraterritorial application, that give government officials sweeping authority to demand sensitive information from Chinese and foreign-owned businesses in the name of state security and other issues of importance to the Chinese Communist Party (CCP). This information may then be used by the CCP to benefit Chinese companies, employed in espionage activities, and weaponized by the People's Liberation Army (PLA). Businesses should take appropriate steps to identify the risks of operating in the PRC's data collection ecosystem.

*Access to Data Through Specific PRC Laws*

To illustrate the risks, take for example the PRC's new Foreign Investment Law (FIL). While the FIL, implemented in January 2020, presents opportunities for foreign investors, including more flexibility on joint venture terms and streamlined entity establishment procedures, the FIL also requires foreign-invested enterprises (FIEs) to follow the PRC's Company Law. This law requires *all* companies registered in the PRC to establish a CCP unit in their Chinese operations and "provide the necessary conditions" for its activities – the FIL expands the prospects for CCP access to the data possessed by such FIEs, their joint venture partners, and the private companies

## Authors

Hon. Nazak Nikakhtar
Partner
202.719.3380
nnikakhtar@wiley.law

## Practice Areas

International Trade
National Security
Privacy, Cyber & Data Governance

with which they might deal.

In addition, the PRC government has enacted a range of interrelated national security laws that impose ill-defined and open-ended obligations on individuals and businesses to provide access, cooperation, or support for the PRC's data accumulation objectives, intelligence operations, and security apparatuses. Among these laws are the PRC's Counter Espionage Law (2014), National Security Law (2015), Counter Terrorism Law (2015), Cybersecurity Law (2016), National Intelligence Law (2017), Encryption Law (2019), and the draft Data Security Law.

As a general matter, these laws compel foreign and domestic firms operating in the PRC or doing business with a company operating in the PRC to share certain data with authorities on request, giving the central government virtually unfettered access to company records and files, business contracts, intellectual property, confidential strategies, and employee and customer personal data. The Counter Espionage Law, National Intelligence Law, and Cybersecurity Law also grant PRC security and intelligence officials the right to enter otherwise restricted business facilities, inspect company records, acquire sensitive data, investigate and question personnel, and seize communications equipment and other property. Under the Cybersecurity Law and Encryption Law, moreover, businesses may be subjected to invasive security audits, requiring the disclosure of source code and other sensitive intellectual property.

Finally, in order to compel businesses to adhere to these and other similar legal mandates, the CCP instituted last year a nationwide social credit rating system for all corporations to detect misconduct and noncompliance. The "Corporate Social Credit System" has implications for companies operating in China (both foreign-owned and domestic) with respect to proprietary technical information, sensitive personal data, and surveillance information. Companies may be given low scores if they fail to transfer their internal data to the CCP as part of their obligations. Failing to score well, by noncompliance with the government's policies or demands, may subject companies to a myriad of sanctions, including higher taxes or permit difficulties, or a blacklisting which could mean financial ruin. The European Chamber of Commerce describes this credit rating system as potentially amounting to "life or death" for companies.

*Business Risks and Reputational Harm*

The PRC government's broad authority to access data has profound implications for businesses. In contrast to U.S. national security laws, which set forth detailed definitions, procedures, limitations, and prohibitions regarding intelligence collection activities, the PRC's national security laws leave key concepts (e.g., "national security," "intelligence," and "counter-espionage" activities) undefined, thereby expanding their potential scope. The non-transparent and often murky justice system in China makes successful litigation – especially litigation against the PRC's central government's actions – nearly impossible. Further, the lack of an extradition treaty with the PRC renders enforcement of U.S. businesses' rights and privacy by the U.S. government exceedingly difficult.

In addition to the legal risks associated with operating in the PRC, there are potentially significant business and financial costs. Foreign businesses risk state-sponsored theft and transfer of their technology and intellectual property to Chinese competitors. They may also risk reputational harm if their data could be used to help the PRC government silence dissent, restrict or censor information, and harass and prosecute human rights defenders and others in the name of state security. Finally, the breadth and complexity of the PRC's national security laws make regulatory compliance especially onerous and expensive for businesses (data localization requirements, for example, may force foreign businesses to make costly investments to duplicate infrastructure and facilities within the PRC).

*U.S. Businesses Should Proactively Self-Monitor*

To fully understand the business and national security risks of operating in the PRC, businesses must be proactive in identifying the sensitive personal and proprietary information in their possession. Businesses should also evaluate the relevant PRC laws and policies which may require government access to data and conduct comprehensive and ongoing due diligence to understand the risks posed by their relationships with PRC companies and their partners. Robust due diligence and transaction monitoring are also critical to understanding potential legal exposure under U.S. laws, including whenever the PRC's demand for data conflicts with U.S. laws. Finally, businesses should develop protocols to respond to PRC authorities' demands for sensitive and proprietary information.