SAFEGUARDING OUR FUTURE

U.S. Business Risk: People's Republic of China (PRC) Laws Expand Beijing's Oversight of Foreign and Domestic Companies

OVERVIEW

Since 2015, the PRC has passed or updated comprehensive national security, cybersecurity, and data privacy laws and regulations, expanding Beijing's oversight of domestic and foreign (including U.S.) companies operating within China. Beijing views inadequate government control of information within China and its outbound flow as a national security risk. These laws provide the PRC government with expanded legal grounds for accessing and controlling data held by U.S. firms in China. U.S. companies and individuals in China could also face penalties for traditional business activities that Beijing deems acts of espionage or for actions that Beijing believes assist foreign sanctions against China. The laws may also compel locally-employed PRC nationals of U.S. firms to assist in PRC intelligence efforts.

LAWS AND THEIR IMPLICATIONS

2023 COUNTER-ESPIONAGE LAW UPDATE

INTENDED PURPOSE:

- Broadens the scope of the PRC's counterespionage law
- Expands the definition of espionage from covering state secrets and intelligence to any documents, data, materials, or items related to national security interests, without defining terms
- Comes into effect 1 July 2023

IMPLICATIONS:

- Potential to create legal risks or uncertainty for foreign companies, journalists, academics, and researchers
- Any documents, data, materials, or items could be considered relevant to PRC national security due to ambiguities in the law

2021 CYBER VULNERABILITY REPORTING LAW

INTENDED PURPOSE:

- Requires all (including U.S.) companies with China-based equities to report cyber vulnerabilities discovered in their systems or software to PRC authorities
- Vulnerabilities cannot be publicly disclosed or shared overseas until PRC authorities complete an assessment

IMPLICATIONS:

- May provide PRC authorities the opportunity to exploit system flaws before cyber vulnerabilities are publicly known

2021 PERSONAL INFORMATION PROTECTION LAW

INTENDED PURPOSE:

- Codifies the privacy rights of PRC citizens
- Requires domestic and foreign (including U.S.) companies to comply with reviews

IMPLICATIONS:

- Controls handling of personal data within and outside mainland PRC when providing products or services to persons within the PRC
- Restricts ability of companies in China to gather and retain personal data
- Authorizes the PRC government to collect personal data for actions Beijing deems to be in the public interest

2021 ANTI-FOREIGN SANCTIONS LAW

INTENDED PURPOSE:

- Provides grounds for the PRC to take countermeasures against foreign sanctions and authorizes PRC actions against foreign persons or entities that implement or assist foreign sanctions against China

IMPLICATIONS:

- Facilitates Beijing's ability to retaliate against foreign entities that it judges have "assisted" in implementing foreign sanctions
- Threshold for assisting in implementing foreign sanctions is unspecified in the law
- May compel U.S. companies to heed PRC regulations rather than U.S. requirements, or face legal consequences

LAWS AND THEIR IMPLICATIONS (CONTINUED)

2021 DATA SECURITY LAW

INTENDED PURPOSE:

- Classifies data in a tiered system according to Beijing's interpretation of the data's importance to state security
- Subjects cross-border data flows to additional regulatory requirements and prohibitions
- Positions Beijing to control or deny cross-border data transfers and refuse foreign government data transfer requests

IMPLICATIONS:

- Expands the PRC's access to, and control of, companies and data within China
- Expands the PRC's ability to control the outbound flow of data
- Imposes stricter penalties on China-based businesses (including U.S.) for noncompliance

2017 NATIONAL INTELLIGENCE LAW

INTENDED PURPOSE:

- Stipulates that citizens or private organizations must assist the PRC's Ministries of Public Security and State Security in national intelligence efforts

IMPLICATIONS:

- Creates "affirmative" legal responsibilities for PRC and foreign (including U.S.) entities to provide access to, or collaborate with, the PRC's intelligence agencies
- May force locally employed PRC nationals of U.S. companies to assist in PRC national intelligence efforts

2017 CYBERSECURITY LAW

INTENDED PURPOSE:

- Outlines PRC's approach to cybersecurity
- Mandates that critical infrastructure companies (undefined in the law) retain their data within China's borders
- Requires data stored in the PRC to be accessible to its intelligence services

IMPLICATIONS:

- Companies must localize certain types of data held within China's borders, including the data of foreign (including U.S.) companies working in undefined critical industries

2015 NATIONAL SECURITY LAW

INTENDED PURPOSE:

- Outlines whole-of-society responsibilities for the PRC's national security posture
- Stipulates that PRC citizens and private organizations must assist the PRC government and intelligence services with security issues when ordered

IMPLICATIONS:

- Mandates that domestic companies and citizens within China provide assistance to all security agencies and assist Beijing on national security issues
- May compel locally employed PRC nationals of U.S. companies to assist in investigations that may expose operating elements of U.S. companies/citizens

This information is current as of 20 June 2023.

This document contains a general overview of certain PRC laws to facilitate discussion and should not be relied upon for legal analysis or treated as legal advice.