Data Security Business Advisory:

Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China

Homeland Security

U.S. Department of Homeland Security
Office of Strategy, Policy, and Plans
Office of Trade and Economic Security

Summary

This Advisory describes the data-related risks American businesses face as a result of the actions of the People's Republic of China (PRC) and outlines steps that businesses can take to mitigate these risks. Businesses expose themselves and their customers to heightened risk when they share sensitive data with firms located in the PRC, or use equipment and software developed by firms with an ownership nexus in the PRC, as well as with firms that have PRC citizens in key leadership and security-focused roles (together, "PRC firms"). Due to PRC legal regimes and known PRC data collection practices, this is particularly true for data service providers and data infrastructure.

The PRC's data collection actions result in numerous risks to U.S. businesses and customers, including: the theft of trade secrets, of intellectual property, and of other confidential business information; violations of U.S. export control laws; violations of U.S. privacy laws; breaches of contractual provisions and terms of service; security and privacy risks to customers and employees; risk of PRC surveillance and tracking of regime critics; and reputational harm to U.S. businesses.

These risks result from direct actions of the Chinese Communist Party (CCP) and from PRC laws that coerce PRC firms into providing data and relevant information to the Chinese government. This Advisory provides an overview of PRC laws and initiatives that compel PRC firms and entities to secretly cooperate with PRC security and intelligence services. These laws may be used to compel PRC firms to illicitly provide the PRC government with data, logical access, encryption keys, and other vital technical information, as well as to install "backdoors" or "bugdoors" in equipment which create security flaws easily exploitable by PRC entities.[2]

This Advisory concludes with recommended actions U.S. businesses can take to address these risks. Businesses that share data with PRC firms or use equipment developed, maintained, or operated by PRC firms should apply due diligence policies and procedures, including consideration of alternative data service providers and equipment. By following these recommendations, businesses can mitigate the data-related risks posed by the PRC and improve the privacy and security of their customers.

1. This advisory is explanatory only and does not carry the force of law. It does not supplement or modify statutory authorities, Executive Orders, or regulations. It is not intended to be, nor should it be interpreted as, comprehensive or as imposing requirements under U.S. law, drawing any legal conclusions about specific fact scenarios regarding particular businesses or entities, or otherwise addressing any particular requirements under applicable law.

Background

The U.S. Department of Homeland Security (DHS) is issuing this Advisory to highlight the risk of PRC government-sponsored data theft. PRC legal regimes enable potential violations of long-standing global norms by allowing for requirements on PRC firms that result in data theft, manipulation, and exploitation in order to further PRC goals.[3] Businesses, individuals, and other persons, particularly academic institutions, research service providers, and investors (hereafter, businesses and individuals) who choose to procure data services and equipment from PRC-linked firms or who store data on software or equipment developed by PRC-linked firms, should be aware of the economic, reputational, and legal risks associated with doing business with these firms.

This Advisory identifies factors that businesses and individuals may consider as part of their data security assessments. It urges businesses and individuals to evaluate their exposures to these risks and to implement due diligence policies, practices, and internal controls. This will ensure their practices are aligned with mitigation of identified risks and international best practices in data security.

In recent years, the PRC has increased its efforts to collect foreign data, through both legal and illegal channels. The CCP's focus on data acquisition supports the goals outlined in the PRC's "Made in China 2025" plan, as well as the Digital Silk Road and the Military Civil Fusion efforts—all of which endeavor to make the PRC the leading global technological superpower by 2049.[4] The PRC has indicated, both directly and through its actions, that data is a high value resource for the next phase of their economic growth.

If oil is the core resource in the era of industrial economy, then data is the most important strategic resource in the era of digital economy."

- PRC National Information Center. March 10, 2020

As part of this plan, the CCP has indicated that it will aid Chinese companies in their efforts to replace foreign companies as engineers, designers, and manufacturers of key emerging and foundational technologies. Through state-sponsored theft of data, such as intellectual property theft and trade secrets, the CCP plans to shift manufacturing from lower-value goods to higher

2. "Backdoor" refers to secret portals purposely added to a system that hackers or intelligence agencies can exploit to gain illicit access to networks."Bugdoor" refers to a backdoor that is made to look like a bug or defect to appear accidental making it more difficult to prove intentional placement.

value-added technical areas. CCP-sponsored data theft not only accelerates the reduction of foreign competitors' domestic market share, it also hastens the arrival of PRC technological dominance in international markets—including in aerospace, semiconductors, robotics, artificial intelligence systems, biometrics, cyber intelligence, genomics, pharmaceutical medicines, and sustainable/green energy materials.

The CCP also collects foreign data to enhance its national security and geopolitical interests. Stolen intellectual property has been essential to the modernization of the People's Liberation Army, equipping it with advanced warfighting and information capabilities. The CCP utilizes foreign data as a tool to map the activities, relationships, status, and vulnerabilities of key individuals, including PRC dissidents. Foreign data collection informs CCP efforts to monitor global sentiments, such as criticism of human rights abuses surrounding the treatment of minority ethnic groups (e.g., Uyghurs or Kazaks) and to develop new propaganda tools and messaging to inject its preferred narratives into global discourse and suppress speech.

- To mitigate related risks to national and economic security, the U.S. Government has taken the following action in response to CCP data theft.
- On August 17, 2017, the United States Trade Representative (USTR) initiated a Section 301 investigation into the CCP's behavior related to forced technology transfer, intellectual property theft, and innovation.
- On May 15, 2019, the President issued an Executive Order on Securing the Information and Communications Technology (ICT) and Services Supply Chain.
- On June 20, 2019, USTR launched a case against China on intellectual property (IP) practices at the World Trade Organization (WTO) and to impose tariffs on $50B of PRC imports, which was later expanded to cover $370B.
- On January 28, 2020, the Department of Justice (DOJ) charged Harvard University's Chemistry Department Chair and two PRC nationals with

3. The PRC has a history of using data acquired illicitly to bolster its own industries. For example, PRC-linked actors illicitly acquired sensitive military information, including information related to the F-35 Joint Strike Fighter program. The PRC leveraged this information in the creation of its own stealth fighter jet, the J-31, and one of the principal thefts of information was sentenced to 46 months in U.S. Federal Prison. https://www.justice.gov/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months

undisclosed research funding, visa fraud, acting as an agent of a foreign government, and smuggling biological research to illicitly aid China's research efforts.

- On February 10, 2020, DOJ charged four People's Liberation Army (PLA) members with hacking into the computer systems of the credit reporting agency Equifax and stealing information of nearly 150 million Americans.
- On February 27, 2020, DOJ announced a PRC scientist was sentenced to 24 months in federal prison for stealing proprietary information worth more than $1 billion from a U.S. petroleum company.
- On March 9, 2020, the President ordered Beijing Shiji Information Technology to divest its interests in StayNTouch, a business that managed hotel guest data, as result of CFIUS investigation.
- On April 4, 2020, the President issued Executive Order 13913 on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, formalizing the mechanism by which federal departments provide risk-based advice to the Federal Communication Commission as it reviews license applications from foreign telecommunications services companies.
- On July 21, 2020, the Federal Bureau of Investigations (FBI) issued an 11-count indictment alleging two Chinese nationals conducted a 10-year hacking campaign, targeting industries in multiple countries.
- On August 6, 2020, the President issued two separate Executive Orders, the first, Executive Order 13942 Addressing the Threat Posed by WeChat and, the second, Executive Order 13943 Addressing the Threat Posed by TikTok.
- On August 11, 2020, a Grand Jury in the District of Columbia indicted several PRC nationals on charges including racketeering, money laundering, fraud, identity theft, and access device fraud stemming from unauthorized computer network intrusions while employed by Chengdu 404 Network Technology Company.

4. For the PRC's Made in China 2025 Press release, see: http://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm. For the Digital Silk Road, see the "Facilities connectivity" section of the PRC's Belt and Road Initiative Action Plan, http://english.www.gov.cn/archive/publications/2015/03/30/content_281475080249035.htm.

PRC Legal and Regulatory System

The PRC government retains the legal and physical capability to compel any Chinese entity or citizen to turn over information. U.S. businesses that associate with entities connected to China place themselves and their customers at risk. The PRC continues to indicate that it will pursue global dominance in its next phase of data-driven technological growth by leveraging its "asymmetrical advantages," which implicitly include the lack of privacy laws, intellectual property rights, and human rights protections.[5]

The PRC National Intelligence Law of 2017: This law forms the baseline of the modern data collection regime, and compels all PRC firms and entities to support, assist, and cooperate with the PRC intelligence services, creating a legal obligation for those entities to turn over data collected abroad and domestically to the PRC. Article 7 of this law states "any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the [National Intelligence] Law, and keep the secrets of the national intelligence work from becoming known to the public."[6] A PRC intelligence agency may request that any PRC firm or entity secretly share access to a U.S. business or individual's data, or otherwise face penalties. In addition, the National Intelligence Law may compel PRC firms to create backdoors and other security vulnerabilities in equipment and software sold abroad so that the PRC government can easily access data not controlled by PRC firms. The law further establishes a system of incentives for compliance and penalties for non-compliance, stating that the PRC "commends and rewards individuals and organizations that have made significant contributions to national intelligence work" and that, "whoever... obstructs the state intelligence work organization and its staff from carrying out intelligence work according to law" shall be dismissed, investigated, and/or detained.

Moreover, a recent series of new laws codify practices that may further perpetuate the illicit acquisition of foreign data. The PRC legal and economic system blurs the line between government and non-government entities by co-opting PRC firms to act as proxies and tools of the CCP. PRC laws also require foreign companies operating in China to store data within the country

5. An example of this can be seen through the PRC's Made in China 2025 plan: https://fas.org/sgp/crs/row/IF10964.pdf.
6. Article 7 of China's National Intelligence Law states, "Any organization or citizen shall support, assist, and cooperate with state intelligence work in accordance with the law, and maintain the secrecy of all knowledge of state intelligence work." (https://www.dni.gov/files/NCSC/documents/news/20190606-NCSC-Remarks-ILTA-Summit_2019.pdf)

and prohibit effective encryption of that data, exposing the data of any U.S. firm or citizen operating within China to potential exploitation and theft.

The PRC Data Security Law of 2020: This law, which is likely to go into effect in early 2021, provides the most recent evidence of the broadening scope of data regulation.[7] Its impending addition to the existing legal framework represents an even greater shift in the CCP's attitude away from protecting Chinese data systems as a defensive mechanism, and toward collecting data as an offensive act. The Data Security Law defines "Data Activities" broadly and with a large scope—to include both activities conducted in China and data-related activities undertaken by organizations and individuals outside of China. The law will focus on data that could harm the country's national security, economic security, social stability or public health.

The Data Security Law indicates that the PRC will establish a centralized process to monitor and assess risk, share data with relevant PRC bodies, and implement a system of early warning for potential data security events. As part of this process, the PRC will institute a national security review to investigate and determine whether companies conduct Data Activities that pose risks to the PRC's national security. It further stipulates that once in effect, the PRC will take countermeasures when other countries take actions the CCP determines to be discriminatory with respect to data-related trade or investments or technologies related to data development and usage. That the law includes this provision—which addresses actions taken in foreign countries that may prevent access by PRC service providers to those markets— signals that the law is not designed solely to protect domestic activities in China, but rather to force foreign markets to remain open to Chinese data services providers. This is a significant contrast to the PRC Cybersecurity Law of 2017.[8]

The Data Security Law will impose multiple obligations upon entities conducting Data Activities including: "to comply with other laws and regulations (like the National Security Law); to favor economic and social development in line with the CCP's social morality and ethics; to enhance risk inspection and reporting to regulatory authorities in case of security

7. In this section we assume the draft law is an accurate approximation of the final law.
8. The PRC Cyber Security Law of 2017 requires businesses operating within China to store business, technological, and personal data on servers located within China and allows Chinese authorities to conduct spot-checks on companies' network operations. The law has a more distinct domestic approach and requires, among other things, network operators in critical sectors to store in the PRC, all data that is gathered or produced in the country.

incidents; to conduct periodic risk assessments; to report the categories, amount, collection, storage, processing, usage of important data, along with security risks and countermeasures; to request data source notification, to review identities of parties, and to keep records by agents of data transactions; to require organizations and individuals to cooperate during evidence collection by police and national security authorities; and to report to Chinese regulatory authorities upon request by regulatory authorities abroad."[9]

Lastly, the Data Security Law will allow CCP authorities to conduct interviews of relevant organizations and individuals to determine whether they are compliant. Organizations and individuals who fail to meet the data security obligations will be subject to warnings, correction orders, and penalties up to 1 million Chinese renminbi (RMB) (approx. $150,000 USD). Moreover, failure to adhere to the new obligations could lead to confiscation of the profits deemed to be connected to the alleged violation, as well as penalties on the individual in charge of the operations. The CCP will make these determinations with no formalized structure, judicial or otherwise, to allow for appeal.

The PRC Cryptography Law of 2020: This law, which went into effect in January 2020, forms the framework for the PRC's domestic encryption control system. The law allows foreign suppliers to provide commercial encryption products only if the systems have been approved and certified by the State Cryptography Administration (SCA). Any encryption system that is "approved" for use in China, or by companies that handle Chinese data, is required to provide its encryption keys to the PRC government. Specifically, Article 31 of the Cryptography Law allows the SCA to request complete access to commercial cryptography systems, including to the data protected by such systems. The result is that the SCA has full access to decryption keys, passwords, and any other information needed to access data on a commercially encrypted server. Therefore, American technology companies must turn over intellectual and technological property if they seek to do business in China.

In addition to expanding its legal framework with these laws, the CCP has begun invoking its Corporate Social Credit System (SCS) to increase its access to business data. Developed to track and regulate corporate behavior in the

9. This sentence refers to the PRC's draft Data Security Law text, a translation of which can be found here: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/.

PRC, the Corporate SCS requires businesses to feed detailed data about their operations and capabilities into a centralized database called the National Credit Information Sharing Platform (NCISP). The data, which may include proprietary data or other sensitive information, is used to evaluate and rate the legal, financial, and civic conduct of businesses and the individuals who run them. The CCP may choose to reward or punish them accordingly. Reports indicate that the Corporate SCS is moving beyond its pilot stages and is on track for at least partial implementation by the end of 2020. According to the U.S.-China Business Council and the EU Chamber of Commerce, multinational firms are already subject to the system's data reporting requirements. Under the Corporate SCS, businesses found by PRC authorities to have engaged in unlawful or illicit behavior (e.g., avoiding CCP-development activities) can be blacklisted and subjected to higher customs fees, more frequent financial audits, and greater market access restrictions (e.g., exclusion from public procurement opportunities). In contrast to U.S. laws, which set forth detailed definitions, procedures,

limitations, and prohibitions regarding intelligence collection activities, PRC laws are extremely broad in scope. PRC laws are developed by the Executive in the absence of either an independent legislature or judiciary. As a result, the purpose of laws in the PRC is essentially to provide justification for the Executive's monopoly of power over the PRC's entities and citizens. PRC laws leave key concepts (e.g., "national security", "intelligence", and "counter-espionage" activities) undefined. Such ambiguity, coupled with a lack of checks and balances within the PRC system regarding implementation and enforcement, makes it difficult for businesses to mitigate legal risk. The absence of an independent judiciary or of other checks within the Chinese system dictates that businesses impacted by these laws have limited to no recourse.

Finally, the breadth and complexity of the PRC's legal framework and Corporate SCS 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).

Risks of Procuring Data Services From, or Partnering with PRC

The PRC legal and regulatory framework around data offers little to no protection to U.S. firms that share data with PRC firms or entities. Businesses and individuals with data exposure to the following vectors, or that are otherwise engaged in data sharing with PRC firms of entities, may face reputational and other risks.

Data Centers Owned or Operated by PRC Firms: PRC laws are most effective at creating compulsory data access when the data travels through a PRC firm abroad or a firm located within the PRC. PRC firms that own and operate data centers, both within China and abroad, are subject to laws which require their secret cooperation with PRC intelligence services. Under this legal framework, these firms are required to secretly share data with the PRC government or other entities upon request, even if that request is illegal under the jurisdiction in which these firms operate.

Foreign Data Centers Built with PRC Equipment: Chinese suppliers are not exempted from PRC laws which require cooperation with PRC intelligence services, even when their equipment leaves the PRC. Under the National Intelligence Law, the PRC has the ability to direct PRC firms to covertly install backdoors or "bug doors" into their equipment or software, allowing for easy access by PRC intelligence services. Additionally, the CCP subsidizes the use of PRC firms hardware, software, telecommunications infrastructure, and other inputs for the creation and operation of data storage and processing centers. This financial advantage allows PRC corporations such as Huawei and ZTE to undercut competitors and to install equipment in a wide array of settings outside the PRC. The spread of such equipment may even affect unwitting U.S. service providers (e.g., where intermediary contracted equipment suppliers have "rebranded" Huawei or ZTE equipment as their own for use in U.S. networks). The CCP subsidies and the spread of PRC-developed equipment not only advantage PRC companies over U.S. providers economically, but also furthers the ongoing capabilities of the CCP where the equipment supplier maintains a service or maintenance contract that necessitates ongoing access.

There are instances where faulty security has been identified in equipment provided by PRC firms, for example, a recent report by the National Cyber Security Centre of Papua New Guinea, which is funded by the Australian Department of Foreign Affairs and

Trade, "assessed with high confidence" that the data center built by Huawei in Papua New Guinea relied on equipment that could easily intercept data flows by entities familiar with the equipment's flaws. The data center used an "openly broken" algorithm for encrypting communications and relied on outdated firewalls that reached their "end of life" two years prior to the facility being opened. Further, Huawei has been predatory when capturing 4G/5G infrastructure deals; in the case of Papua New Guinea, Huawei offered a deal that was nearly 30% under market value, then proceeded to change the agreement two years later. In addition, operators for the telecommunications firm Telikom PNG admitted that they could not see 20-30% of the network traffic, and all changes needed to be vetted by a Huawei employee. Finally, the Service Level Agreement (SLA) precluded technology outside of Huawei's ownership from being brought onto the network infrastructure while operational language of manuals only appeared in Mandarin Chinese, further reinforcing monopolization concerns and hindering the ability to operate equipment without direct Huawei assistance.

Joint Ventures: Under the PRC legal framework, the PRC government may request secret access to any data to which a PRC firm or entity is provided access, whether as a Joint Venture (JV) partner or through other data sharing agreements. This legal requirement applies regardless of the legal jurisdiction of the JV. This is important for JVs who gather or maintain third-party data for which they have made assurances of privacy and confidentiality.

Legally Acquired Data Augmenting Illicitly Acquired Data: The CCP, or agents working on its behalf, can also purchase data through brokers to augment and validate illicitly acquired data. Combinations of incomplete or anonymized data, when layered on top of each other, can create a more complete data set for identification and analysis. In many cases, anonymized data sets require only a few additional "anonymized" data elements to make identification possible, even though each data set had been gathered independently under current practices for anonymization. Matching data elements across licitly and illicitly acquired data sets—especially if combined with methods to identify and link data to specific devices via media access control (MAC) address, browser fingerprinting,

or other method—increases the risks to U.S. entities for storing or analyzing anonymized or incomplete data with companies that have a PRC nexus.

Software and Mobile Device Applications: Data collected through software and mobile applications owned or operated by PRC firms is also accessible to the PRC government through its legal system. These programs have the ability to collect and transmit data stored anywhere on the host device, particularly when they are granted unrestricted access—a default setting with which many mobile and computer apps come preprogrammed. For example, the United States government provided evidence that the Chinese app TikTok has violated its own terms of service and circumvented protections built into the Android operating systems to covertly track a device's unique MAC address. This type of data, combined with app usage and location data, enables the creation of a real-time relational mapping and tracking capability. TikTok has also allegedly exploited flaws in Apple iOS to discover information stored by the user in the clipboard function of the iOS operating system.

Fitness Trackers and Other Wearables: Even where the identity of the wearer is kept anonymous by the device itself, the combination of location data over a certain time interval can identify where each user lives, works, or otherwise spends time. Location data of this sort would not only provide travel patterns of wearers, but—in combination with property tax records—could be further leveraged to identify names and family members. The CCP could obtain this data by requesting it from fitness tracker and wearables companies that operate inside of the PRC under the National Intelligence Law and the the PRC. Where the potential path of dataflow is unknown, strong encryption provided by a company that does not operate within the PRC should be used.

Recommended Actions

Businesses and individuals that operate in the PRC or with PRC firms or entities should scrutinize any business relationship that provides access to data—whether business confidential, trade secrets, customer personally identifiable information (PII), or other sensitive information. Businesses should identify the sensitive personal and proprietary information in their possession. To the extent possible, they should minimize the amount of at-risk data being stored and used in the PRC or in places accessible by PRC authorities. Robust due diligence and transaction monitoring are also critical for addressing potential legal exposure, reputation risks, and unfair advantage that data and intellectual property theft would provide competitors. Businesses should seek to acquire a thorough understanding of the ownership of data service providers, location of data infrastructure, and any tangential foreign business relationships and significant foreign investors.

Terms of Service/Contractual Agreements should explicitly state where data is stored, who has access to it, and how liability is allocated in the event of a failure to adhere to legal requirements. Choice of law, forum selection, and arbitration clauses should list a trusted jurisdiction outside of the PRC. Where the potential path of dataflow is unknown, strong encryption provided by a company that does not operate within the PRC should be used.

For the most sensitive data, an additional risk-mitigating step would be to seek out well-known alternative service and equipment providers. Determination of whether a supplier is "trustworthy" should occur through rigorous evaluation which considers the rule of law; the security environment; ethical supplier practices; and a supplier's compliance with security standards and industry best practices. The following list provides examples of the types of data that should be considered particularly sensitive:

1. Technology and other data in connection to export-controlled products.
2. Intellectual property, including trade secrets, relating to emerging technologies identified in China 2025 and other PRC plans.
3. Biotech, genomic data, and medical test data.

4. Personally-identifiable and other sensitive information.
5. Geolocation data.[10]

Organizations should remain alert when conducting business in China, and IT operators should ensure proper segmentation of their network infrastructure from any external software use. In addition, businesses operating in the PRC should develop protocols to respond to PRC authorities' demands for potentially sensitive information. In particular, U.S. businesses should notify the legal attaché at the U.S. Embassy in Beijing upon receipt of any such demand.

U.S. businesses are advised to implement appropriate cyber security safeguards. Cyber security is an iterative process that requires businesses to identify, detect, and prioritize risks to networks and to adjust their safeguards on an ongoing basis. Businesses should familiarize themselves with the Cybersecurity Framework published by the National Institute of Standards and Technology (NIST), a voluntary framework that includes standards, guidelines, and best practices to manage cybersecurity risk. These mitigation actions are not comprehensive but will be helpful as part of a multilayered data security policy.

10. The CCP is using global demand for COVID-19 testing to gather genomic data through services offered by Beijing Genomics Institute (BGI). Many countries from which the PRC government is gathering this data have privacy laws in place that prevent domestic companies from using DNA information to develop genomic and personalized medicine at scale. The CCP, however, does not exclude or protect DNA data. Thus BGI—which already has over 10 million sequences in its DNA bank—is rapidly scaling up. This DNA banking effort is already widespread in China and has expanded from its prior scope of tracking Uyghurs in Xinjiang.

Homeland Security

WITH HONOR AND INTEGRITY, WE WILL
SAFEGUARD THE AMERICAN PEOPLE, OUR
HOMELAND, AND OUR VALUES

www.dhs.gov