Skadden

Privacy & Cybersecurity Update

Chinese Cybersecurity Law Goes Into Effect Despite Ongoing International Criticism

China's new cybersecurity law, which has been controversial since its initial draft publication, has now gone into effect with international parties grappling with how it will be implemented.

On June 1, 2017, the new Chinese cybersecurity law became effective, despite persistent pushback from both the international business community and rights organizations. The law, which was first published as a draft in July 2015, will apply to the construction, operation, maintenance and use of information networks in China, as well as the supervision and management of network security within China. The broad, sweeping regulations grant the Chinese government increased centralized power to "ensure network security, to safeguard cyberspace sovereignty, national security and the societal public interest," according to language distributed by the government.

Following the approval of the law by the Standing Committee of China's National People's Congress in November 2016, multinational business organizations primarily have criticized the breadth and vagueness of key provisions, suggesting that parts of the new law will make it difficult, if not impossible, for them to operate in China, or, at the very least, make it significantly more expensive for them to do so. Analysts also have suggested that the law's vagueness indicates that the Cyberspace Administration of China will have broad latitude to direct how the law is interpreted and enforced. The Computer & Communications Industry Association (CCIA), an international nonprofit that represents the computer, internet, information technology and telecommunications industries, has cautioned that the new law could harm trade, and has pointed to a number of the law's more troubling provisions, including vague data-localization requirements and broad obligations relating to data sharing, technical assistance and security reviews. The CCIA has gone as far as implying that China's new cybersecurity rules could violate its World Trade Organization commitments.

Overall, confusion about the law has caused some institutions and organizations, such as the CCIA, to delay the law's implementation pending further guidance from the Chinese government. Partially in response to a call from a collection of business lobby groups representing European and Asian firms and pressure from the European Union Chamber of Commerce in China, the Cyberspace Administration of China reportedly will delay rules governing cross-border data flow, which is slated to take effect at the end of 2018.

Key Provisions

The new law places increased obligations on three types of entities conducting business in China: (1) critical information infrastructure operators, (2) network operators, and (3) network products and services providers.

Critical Information Infrastructure Operators

The law imposes a number of new requirements on entities that are critical information infrastructure operators. However, the definition of such entities is vague, making those new requirements applicable to any number of companies. Under the terms of the new law, critical information infrastructure includes "public communication and information services, power, traffic, water, finance, public service, electronic governance and other critical information infrastructure that if destroyed, losing function or leaking data might seriously endanger national security, national welfare and the people's livelihood, or the public interest, on the basis of their tiered protection system." As provided in Article 37, companies deemed critical information infrastructure operators are required to store, within mainland China, any personal information and "other important data" — currently undefined by the new law — gathered or produced during operations. The law provides one exception to its data localization requirement, namely where a business requirement to share such data outside of China is "truly necessary." However, what qualifies as "truly necessary" remains undefined, and companies seeking reprieve under this exception would still have to submit to a security assessment, which some have noted may require companies to disclose sensitive information to the government. An earlier draft of the law suggested that disclosure of source code would be required as part of the security assessment, but the reference was removed following protests from other countries.

Network Operators

Under the new law, broad obligations also are placed on network operators, which are defined as "network owners, managers and network service providers." Network operators are expected to adhere to social mores, commercial ethics and to "accept supervision from the government and public." What is meant by "supervision from the government" is currently unclear. Moreover, network operators that provide "network access and domain registration services for users, phone network access or provide users with information publication or instant messaging services" must require their users to provide "real identity information." Pursuant to Article 28, network operators also should be prepared to provide "technical support" to public security and state security organizations to aid in their efforts to preserve national security and investigate crimes. The law has not defined what is contemplated by "technical support." However, critics have speculated that this support obligation could mean turning over personal data or encryption keys to the Chinese government. The new law also offers increased protection to data subjects, at least as such protection relates to their internet service providers, if not the Chinese government. Without data subject consent, network operators must not provide personal information to third parties, unless the data subject is "unidentifiable and cannot be recovered." Under the new rules, data subjects have the ability to correct flawed personal information and may have such information deleted if the network operator "violated the provisions of laws, administrative regulations or agreements between the parties to gather or use their personal information."

Network Products and Services Providers

For providers of network products and services, the new law obligates such entities to inform users and "competent departments" whenever a security flaw or vulnerability is discovered. The new law specifically highlights "critical network equipment" and "specialized network security products," which either must meet certification standards or safety inspection requirements before being sold on the Chinese market. The law does not specify such standards or requirements.

Penalties for Noncompliance

The law provides for a number of enforcement mechanisms that can be invoked against companies and individuals for violating the law, depending on the nature of the violation. Regulators can shut down websites, freeze assets and revoke business licenses, and, in some cases, individuals may be detained for up to 15 days. Fines also may be imposed on companies or management personnel ranging from approximately $7,500 to $150,000, and against individuals ranging from approximately $750 to $15,000.

Related Measures: 'Measures for the Security Assessment of Outbound Transmission of Personal Information and Critical Data'

On April 11, 2017, the Cyberspace Administration of China released a draft article titled "Measures for the Security Assessment of Outbound Transmission of Personal Information and Critical Data," which outlines measures requiring firms exporting certain personal and important data to undergo annual security assessments as part of their obligations under the new Chinese cybersecurity law. The draft article contemplates two types of security assessments: (1) self-assessments and (2) assessments conducted by a competent authority. "Network operators" must conduct self-assessments before transmitting critical data or personal information outside of China. However, a security assessment must be submitted to, and conducted by, the competent authority under the following outbound data transfer circumstances:

- the transfer is more than 1000 gigabytes of data;
- the data transfer affects more than 500,000 users;
- the transfer involves data related to sensitive geographic and ecological data, nuclear facilities, chemistry, biology, national defense and the military, the marine environment or population health; or
- the transfer involves data relating to information about the cybersecurity of key information infrastructure, such as system vulnerabilities and security protection.

It appears that all outbound transfers made by critical information infrastructure operators are subject to security assessments. Moreover, the draft article would ban the export of economic, technological or scientific data, if such a transfer would pose a threat to security or public interests. The draft article would require businesses to obtain the consent of users before transferring personal data overseas, a requirement that, in some ways, is similar to the requirements under the EU General Data Protection Regulation that will go into effect in 2018.

On May 27, 2017, the National Information Security Standardization Technical Committee of China published draft guidelines, titled "Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment," to complement and elaborate upon the cross-border security assessment requirements. The guidelines, which are open for public comment until June 26, 2017, indicate that officials will take a risk-based approach to conducting security assessments and analyzing transfers. Generally, outbound transfers must be lawful and legitimate, and it appears that transfers conducted for genuine business purposes would satisfy this low standard. Once a transfer meets this threshold, officials will assess an assortment of risk factors including the features of the data to be transferred and the likelihood of a security incident. Regulators also will look at a company's own data protection plan, and the political and legal environment of the country in which the data recipient is located. In addition to outlining the risk factor calculus for security assessments, the guidelines also provide some clarity on what is considered to be "important data." The guidelines include an annex, delineated sector-by-sector, with examples of what regulators would consider as important data. However, this analysis ultimately remains likely to be on a case-by-case basis.

Key Takeaways

Given the law's broad definitions of entities to which it applies, and the broad obligations it would impose, companies in numerous fields may find themselves swept up into this new law and subject to additional requirements. It is anticipated that Chinese government agencies and industry organizations will issue more detailed implementation regulations and standards, which may provide further guidance to companies that would be subject to the new law.

Return to Table of Contents

Colorado Establishes Cybersecurity Rules For Broker-Dealers and Investment Advisers

Colorado has followed in the footsteps of New York by adopting new cybersecurity rules to which broker-dealers and investment advisers must comply. The rules were proposed by the Colorado Division of Securities (the division) roughly one month after New York adopted similar financial institution regulations.[1] The division's final rules were adopted on May 19, 2017, and will take effect on July 15, 2017.

Colorado adopted two separate rules — one for broker-dealers and one for investment advisers — each of which focus on requirements related to storing and safeguarding electronic financial information. Under the rules, for example, broker-dealers and investment advisers must include cybersecurity in their annual risk assessments and implement "reasonably designed" cybersecurity procedures. These procedures, if reasonably possible, should include: (1) an annual assessment of potential risks to confidentiality, integrity and availability

[1] See our February 2017 *Privacy & Cybersecurity Update*.

of Confidential Personal Information; (2) use of secure email, including encryption and digital signatures, for messages containing Confidential Personal Information; (3) methods to authenticate electronic client instructions; (4) methods to authenticate employee access to electronic communications, databases and media; and (5) disclosure to clients about the risks of using electronic communications.

Whether these procedures are reasonable will depend on factors relevant to the particular firm at issue, including: size; relationship with third parties; policies, procedures and training of employees with regard to cybersecurity; authentication practices; use of electronic communications; automatic locking of devices with access to Confidential Personal Information; and the process for reporting lost or stolen devices.

The definition of Confidential Personal Information in this context is similar to that for personal information in the security breach notification provision of the Colorado Consumer Protection Act, namely, first and last name coupled with any of the following: (1) social security number, (2) driver's license or identification card number, or (3) financial account number or credit or debit card number, in combination with any required security or access code or password that would permit access to a resident's account. In addition, electronic signatures, usernames and passwords are treated as Confidential Personal Information. Generally, data breach notification laws passed in recent years have trended toward including more types of digital information in their definitions of personal information, as the use of online platforms for services involving personal information has proliferated.

Key Takeaways

Before these actions by New York and Colorado, regulation of data security in the financial services industry was mostly under the purview of federal agencies like FINRA and the SEC. After this most recent set of state rules goes into effect, the Colorado securities commissioner will have the ability to bring enforcement actions for subpar cybersecurity procedures. Additionally, the new rules may serve as important "standard of care" guidelines in data breach fiduciary duty and negligence claims. Even with these additional litigation and enforcement possibilities, the new division rules likely will impose relatively light burdens on firms who already are complying with federal guidance.

Return to Table of Contents

Treasury Report Examining Financial Regulatory System Emphasizes Need for Better Coordination on Cybersecurity Regulation

The Treasury Department has issued a report calling for federal and state regulators to coordinate on cybersecurity.

On June 12, 2017, the U.S. Department of Treasury released "A Financial System that Creates Economic Opportunities: Banks and Credit Unions," the first in a series of reports to President Trump examining the financial regulatory system[2] (the report). The report proposes various reforms to the financial regulatory system. One of two themes on which the report focused was the need for better coordination of cybersecurity regulation. If the report's proposals are implemented, government oversight of cybersecurity could become more streamlined.

The report recognizes the critical role that cybersecurity plays in financial regulation, noting that financial institutions and regulatory agencies share the same goal of "maintaining the safety and soundness of the financial system by mitigating and protecting financial institutions and the sector from cybersecurity risks." In order to achieve this goal and ensure the efficiency and effectiveness of the regulatory framework, the report called for federal and state regulators to work together to better coordinate cybersecurity regulation, aided by the Financial and Banking Information Infrastructure Committee.[3] In particular, the Department of Treasury highlighted the need for financial regulatory agencies to harmonize regulations (including by using a common lexicon), interpretations and implementation of specific rules and guidance pertaining to cybersecurity. The report also recommended that federal and state agencies "establish processes for coordinating regulatory tools and examinations across sub-sectors."

Return to Table of Contents

[2] The report can be read here.

[3] The FBIIC is a standing committee chartered under the president's Working Group on Financial Markets consisting of 18 federal agencies and state membership organizations charged with coordinating efforts to improve the reliability and security of the financial sector's infrastructure.

Supreme Court Grants *Certiorari* in Sixth Circuit Cell-Site Location Information Case

The U.S. Supreme Court has granted a writ of *certiorari* in *United States v. Carpenter*,[4] a decision that could provide insight into how location data should be treated from a privacy perspective.

On June 5, 2017, the U.S. Supreme Court granted cert. in *United States v. Carpenter*, a case that concerns whether a warrant is required under the Fourth Amendment in order for the government to access historical cell-site location records held by service providers. At issue is the scope of one's right to privacy in data that reveals the location and movements of a cellphone.

Background

In April 2011, the FBI arrested four men in connection with a series of armed robberies. One of the men confessed and provided phone numbers for the other participants. Without a warrant, the FBI then obtained cell-site location information[5] (CSLI) records for two suspects, Timothy Carpenter and Timothy Sanders. The records pertaining to Carpenter contained 12,898 separate points of location data collected over 128 days, and the records pertaining to Sanders contained 23,034 separate points of location collected over 88 days.

The government later charged Carpenter and Sanders in connection with the robberies. Before trial, Carpenter and Sanders filed a motion to suppress the CSLI evidence on grounds that the Fourth Amendment required the FBI to obtain a warrant supported by probable cause. The motion was denied, and Carpenter and Sanders were convicted at trial, based in part on the CSLI records. After their convictions, Carpenter and Sanders appealed to the Sixth Circuit Court of Appeals. The American Civil Liberties Union, alongside the Brennan Center, Center for Democracy & Technology and other organizations, filed an *amicus* brief arguing that the government violated the Fourth Amendment when it obtained the location records from the defendants' wireless carriers without a warrant.

On April 13, 2016, the Sixth Circuit concluded that the historical CSLI in this case was not protected by the Fourth Amendment.[6] As a result, Carpenter and Sanders petitioned for *certiorari*.

Related Location Data Issues

The *Carpenter* case is the latest development in a series of cases and regulatory reports on the scope of privacy protection for geolocation data:

- In 2017, the Federal Trade Commission (FTC) released a staff report on Cross-Device Tracking, recommending that companies refrain from collecting and sharing precise geolocation information without consumers' affirmative express consent.[7]
- In 2016, the Federal Communications Commission adopted rules that require internet service providers to obtain affirmative "opt-in" consent from consumers to use and share sensitive information, including precise geolocation data.
- In 2016, the FTC sued InMobi Pte Ltd. for its mobile app practices. Although the case was settled, the complaint revealed that the FTC believes: (1) inferential geolocation determinations, to a certain level of specificity, are unlawful; (2) geolocation data is personal information under the Children's Online Privacy Protection Act, thus triggering notice and consent requirements under the act; and (3) "location information" includes information about a consumer's location that is collected through an application programming interface, as well as information that is "inferred from any other data collected through an application programming interface, including but not limited to Basic Service Set Identifiers, with the limited exception of Internet Protocol addresses used to infer location at no greater accuracy than city-level."

Key Takeaways

While the *Carpenter* case relates to Fourth Amendment protection of geolocation data, the court's decision may provide valuable insight into how the court views this increasingly important piece of personal data.

Return to Table of Contents

[4] *U.S. v. Carpenter*, 819 F.3d 880 (Sixth Cir. 2016), cert. granted, 2017 WL 2407484 (June 5, 2017). A copy of the Sixth Circuit opinion may be found here.

[5] Cell-site location information is a phone company record of cellphone towers a given phone connects to at a given time and date. Note that CSLI is less precise than GPS location.

[6] The majority found that the CSLI is unprotected because it deals with routing or conveying information, not the content of the related communications. The majority also cited other reasons, including the Third Party Doctrine.

[7] Find a copy of the report here.

Contacts in the Cybersecurity and Privacy Group

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Lisa Gilford
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

Ivan Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

Jen Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

William Ridgway
Counsel / Chicago
312.407.0449
william.ridgway@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000