ALERT MEMORANDUM

Understanding the Impact of China's Far-Reaching New Cybersecurity Law

October 5, 2017

As the implementation of China's first comprehensive cybersecurity law[1] (the "CCL") progresses, concern is mounting in the international business community regarding the law's expansive scope, prescriptive requirements and lack of clarity on a range of critical issues. Vocalizing such concern, on September 25, 2017, the United States government asked China to halt its implementation of the CCL and highlighted potential issues with the CCL to members of the World Trade Organization. The CCL, officially entitled the PRC Network Security Law, was adopted in November 2016 with the stated goal of protecting Chinese cyberspace sovereignty and ensuring network security within China. Since its passage, several regulations have been released by the principal agency responsible for its implementation, the Cyberspace Administration of China (the "CAC").[2] These regulations were intended to implement the provisions of the CCL, but in some cases appear to have further expanded its scope while leaving some critical questions unanswered. In the face of such uncertainties, foreign companies operating in China are advised to familiarize themselves with the requirements of the CCL and its implementation rules and adopt measures to enhance their preparedness for the full implementation of the CCL.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors:

BEIJING

Ling Huang
+86 10 5920 1090
lhuang@cgsh.com

NEW YORK

Daniel Ilan
+1 212 225 2415
dilan@cgsh.com

Zheng (Jonathan) Zhou
+1 212 225 2006
zzhou@cgsh.com

WASHINGTON

Katherine Mooney Carroll
+1 202 974 1584
kcarroll@cgsh.com

[1] Prior to passage of the CCL, China had passed some cybersecurity regulations in areas such as data protection and telecommunications services, including: "*Measures for the Administration Communication Network Security Protection*" (effective since 2010), "*PRC Regulations for Safety Protection of Computer Information Systems*" (as amended in 2011), "*PRC Regulation on Internet Information Service*" (as amended in 2011), "*Provisions on Protecting the Personal Information of Telecommunications and Internet Users*" (effective since 2013) and the "*PRC National Security Law*" (effective since 2015).

[2] On April 11, 2017, the CAC released the draft *Measures for the Security Assessment of Cross-border Data Transfer of Personal Information and Important Data* (the "Draft Data Transfer Measures") for public comment until May 11, 2017. On May 2, 2017, the CAC released the following two regulations, each with an effective date of June 1, 2017: (1) the *Measures for the Security Assessment of Network Products and Services (for Trial Implementation)* (the "Trial Network Product Measures"); and (2) the *Measures for the Regulation of Internet News and Information Services* (the "Information Services Measures"). On July 10, 2017, the CAC released the draft *Regulations on Protection of Critical Information Infrastructure Security* (the "Draft CII Regulations") for public comment until August 10, 2017. On May 2, 2017, the CAC also released the *Rules for the Administrative and Enforcement Procedures for Internet Information and Content Management*, effective June 1, 2017, which primarily regulate procedural matters in administrative penalty cases involving internet information content.

I. Overview: Scope of the CCL and the Implementing Regulations

The scope of the CCL is extremely broad, applying to the construction, operation, maintenance and usage of networks, as well as network security supervision and management within the territory of the People's Republic of China ("China").[3]

A. *Covered Entities*

Most of the obligations are specifically imposed on "network operators," a term that is defined expansively to include owners and administrators of networks[4] and network service providers, and thus would likely include not only internet and technology companies, but financial institutions and other companies that use networks to provide services to customers.

B. *Territorial Scope*

The CCL makes no distinction among domestic and foreign network operators. Thus, the CCL will apply to both domestic and foreign entities operating networks or using networks to provide services to customers in China. Additionally, while the CCL's primary purpose is to regulate network-related activities within China, in accordance with the CCL's stated intent to protect cyberspace sovereignty (meaning China's right to regulate the transmission of data within its borders), the CCL will have implications for Chinese and foreign-owned entities operating outside of China. For example, the CCL authorizes governmental agencies to block transmission into China of information originating outside of China if those transmissions violate a Chinese law or regulation. In this respect, China represents one of a growing number of significant jurisdictions seeking to impose territorial regulation on internet content and services, creating significant challenges given the global nature of the internet.

C. *Subject Matter Scope*

The CCL imposes obligations in multiple areas, including with respect to network security, procurement of network products and provision of network services, protection of critical information infrastructure, local data storage, cross-border data transfers and the protection of "personal information."

II. Key Provisions of the CCL and Certain Implementing Regulations

A. *Network Security Obligations Imposed on Network Operators*

— *Tiered System of Basic Cybersecurity Obligations*

Article 21 of the CCL imposes the following set of basic cybersecurity obligations on network operators: (1) formulating internal security management systems and operating rules, and assigning a responsible individual for network security to implement network security protection measures; (2) adopting technological measures to prevent network attacks and other actions that could endanger network security; (3) adopting technological measures to monitor and record network operational statuses and security incidents and preserving relevant network logs for at least six months; and (4) adopting other measures to protect data, such as data classification, backup of important information and encryption. The performance of such obligations will be based on a "tiered system for network security protection." Under such a "tiered system," operators of networks belonging to a higher tier in terms of network security concerns will likely be subject to more stringent requirements and heightened obligations. The details of such tiered system will be subject to future rulemaking.

— *Additional Obligations*

In addition to the tiered set of basic obligations in Article 21, network operators are also subject to a wide range of other obligations under the CCL, which do

[3] Based on Chinese legal norms, "territory of the People's Republic of China" is thought to generally exclude Hong Kong, Macau and Taiwan.

[4] "Network" is defined as systems that consist of computers or other information terminals and the relevant facilities, which are used for collecting, storing, transmitting, exchanging and processing information.

not appear to be subject to the tiered system for compliance. In particular:

- Vulnerability Reporting: network operators must report to relevant governmental agencies any "security flaw or vulnerability" and any network security breach (Articles 22 and 25);
- Assistance to Government: network operators must provide technical support and assistance to relevant governmental agencies' criminal investigations or national security activities (Article 28);
- User Authentication: network operators who provide networking services to users (such as network access, domain name registration or fixed-line or mobile telephone access) or who provide users with instant messaging or information publication services (e.g., the ability to post in online forums) are required to use authentication techniques to identify users and must refuse to provide service to any user who does not provide the relevant authentication information (Article 24); and
- Mandatory Safety Certification: network operators may not provide or sell "critical network equipment" or "specialized network security products" before undergoing a safety inspection and certification by qualified institutions. The CCL states that the applicable equipment and products will be published in a catalog (Article 23). On June 1, 2017, the CAC, jointly with the Ministry of Industry and Information Technology ("MIIT"), the Public Security Bureau ("PSB") and the State Certification and Accreditation Administration ("CAA"), published the *First Catalog of Critical Network Equipment and Specialized Network Security Products* (the "First Catalog"). A total of fifteen (15) products[5] were included on the First Catalog. According to the First Catalog, a qualified institution is one that is jointly certified by the CAC, MIIT, CAA and PSB according to relevant rules and regulations.

— *Impact on Foreign Companies Operating in China*

The impact of the tiered system on foreign companies operating in China will not be known until the rules regarding the tiered system are promulgated. The CCL does not specify which agency has the responsibility to promulgate relevant rules for the tiered system for compliance. In addition, it is not clear whether such system will be modeled after, or even based on, existing tiered systems for network protection (on computer information system information security and communication network safety, respectively). Further, it remains to be seen whether such foreign companies are disproportionately assigned to a higher tier, resulting in more stringent obligations, and what additional obligations may be imposed on network operators belonging to a higher tier. The impact of the non-tiered provisions on foreign companies depends on the extent to which such foreign companies are already doing what is required by the CCL, but what is seemingly certain is that the tiered and non-tiered provisions will increase companies' compliance costs.

In addition, foreign companies operating in China should closely review the First Catalog and any future catalogs of "critical network equipment" and "specialized network security products," as the safety certification process may significantly delay the going-to-market of such equipment and products and result in the disclosure to the certification institution of certain sensitive information (such as trade secrets) relating to such equipment and products. The First Catalog did not specify the criteria for inclusion in the catalog, so it remains to be seen what other critical

[5] The following four products meeting the prescribed specifications are deemed critical network equipment: certain routers, certain switches, certain services (rack mounted) and certain programmable logic controllers. The following eleven (11) products meeting the prescribed specifications are deemed specialized network security products: certain integrated data backup equipment, certain hardware for firewalls, certain web application firewalls, certain intrusion detection systems, certain intrusion defense systems, certain security isolation and information exchange products (gatekeeper), certain anti-spam mail products, certain network synthetic audit systems, certain network vulnerability scanning products, certain security data systems and certain website recovery products (hardware).

network equipment and specialized network security products may be added to any further catalogs. Furthermore, the procedures, timeline and scope of the mandatory safety certification have not yet been promulgated.

B. *Heightened Security Obligations for Operators of "Critical Information Infrastructure"*

The CCL subjects operators of "critical information infrastructure" to heightened obligations. The CCL stipulates that the scope of critical information infrastructure and detailed rules for its protection will be promulgated by the State Council. The Draft CII Regulations represent the first major implementing regulation with respect to the protection of critical information infrastructure. As described below, they provide greater detail on the scope of critical information infrastructure and the obligations of operators of critical information infrastructure.

— *Critical Information Infrastructure – (Un)Defined*

Critical information infrastructure, a new concept in Chinese law, is defined in Article 31 as infrastructure (1) that is used in public communications and information services, energy, transportation, water conservancy, finance, public services or electronic governance or (2) that, if it were destroyed, malfunctioned or leaked data, could seriously endanger national security, national welfare and the people's livelihood or the public interest. This definition has raised significant uncertainty around a key concept that has important consequences under the CCL. The Draft CII Regulations seek to provide greater details with respect to the scope of critical information infrastructure but still do not provide much clarity. According to Article 18 of the Draft CII Regulations, a network facility or information system would constitute critical information infrastructure if it is operated or managed by any entity in a greatly expanded list of industries and sectors, including finance, transportation, telecoms, internet, cloud computing and big data services, provided that the "serious endangerment" test set forth in (2) above is met (national security national welfare and the people's livelihood or the public interest could be seriously endangered in the event such facility or system is destroyed, malfunctions or suffers a data leakage).[6]

While, as noted above, the Draft CII Regulations significantly expand the industries explicitly included in the scope of critical information infrastructure, by providing a non-exhaustive list of industries, they still leave open the possibility that entities operating in an industry not specifically enumerated could also be deemed to operate a critical information infrastructure if the serious endangerment test is met. Therefore, the Draft CII Regulations leave significant ambiguity about the scope of critical information infrastructure. Anticipating further rulemaking, Article 19 of the Draft CII Regulations stipulates that the CAC, together with telecommunications regulators and PSB, will promulgate guidelines for the identification of critical information infrastructure. It remains to be seen if such guidelines will provide a more definitive delineation of the scope of critical information infrastructure.

— *Additional Network Safety Obligations Imposed on Operators of Critical Information Infrastructure*

The CCL imposes additional network safety and security obligations on the operators of critical information infrastructure, which are also based on the tiered system for network security protection described in Section II.A., including:

- Additional Security Obligations: such as (1) setting up specialized security management bodies and persons responsible for security management and conducting security background checks on the responsible persons and personnel appointed to critical positions;

[6] The industries and sectors enumerated in the Draft CII Regulations are: governmental agencies, energy, finance, transportation, water conservancy, health care, education, social security, environmental protection, public utilities, telecommunications networks, broadcast networks, internet, entities providing cloud computing, big data and other large scale public information network services, national defense, heavy equipment, chemical industry, food and drug industry, radio stations, TV stations, news press and "others."

(2) periodically conducting network security education, technical training and skills evaluations for employees; (3) conducting disaster recovery backups of important systems and databases; and (4) formulating emergency response plans for network security incidents and periodically organizing drills.

- Annual Safety Review and Report Filing: Article 38 requires that the operator of critical information infrastructure conduct a self-evaluation regarding its network safety and potential risks at least annually and file the evaluation report and proposed improvement measures to the relevant governmental agencies.
- Qualified Personnel: Article 26 of the Draft CII Regulations requires that all key personnel in the operation of a critical information infrastructure must first obtain a credential (rules for the issuance of credentials will be promulgated in the future) before taking the position.

— *Impact*

As with the definition of "network operator," the current definition of critical information infrastructure in the CCL and the Draft CII Regulations could potentially ensnare a large number of companies that are not in the internet/technology industry (e.g., financial services companies). Given the uncertainty as to who is an operator of critical information infrastructure, companies will find it difficult to determine which obligations apply to their operations. For some global enterprises, they will already comply with many of these obligations as a matter of best practices, but some companies will, at minimum, need to impose greater formality in their policies and procedures. The requirement to file a self-evaluation report with the relevant Chinese governmental agency will likely raise the most questions and concerns for foreign companies. Companies operating in sectors enumerated in Article 31 of the CCL and/or Article 18 of the Draft CII Regulations that cannot be certain whether they are operators of critical information infrastructure may conclude that it is prudent to comply with the additional obligations described above or consult with counsel to gauge what action, if any, needs to be taken.

C. *National Security Clearance for Purchasing Network Products and Services*

— *Initial Scope of the Law*

Article 35 of the CCL states that if an operator of critical information infrastructure purchases network products and services that may affect national security, then the products or services purchased must be subject to national security clearance conducted by China's network information authorities and relevant departments of the State Council (hereinafter, "cybersecurity review"). The cybersecurity review is focused on whether the network products and services concerned are "secure and controllable," including with respect to data security and the ability to prevent their exploitation for illegally collecting, storing, processing or using users' data.

— *Potential Expansion of the Law's Scope through Implementing Regulations*

The Trial Network Product Measures, effective as of June 1, 2017, aim to implement Article 35, but provide a different standard for their scope of application that may broaden the applicability of cybersecurity reviews. Specifically, the Trial Network Product Measures provide that procurement of "important network products and services" for network and information systems that may affect China's national security will be subject to cybersecurity review, irrespective of whether the procuring entity is an operator of critical information infrastructure. By contrast, Article 35 only requires cybersecurity review of procurement by an operator of critical information infrastructure. The Trial Network Product Measures do not clarify what constitutes "important network products and services," and it is not clear how the determination of whether network products or services may affect national security will be made.

— *Impact*

While details of the cybersecurity review, particularly the standards, timing and procedures that are applicable in the review process, are subject to

future rulemaking, it is worth noting that the mere requirement of cybersecurity review for procurement could, in practice, favor products made by Chinese suppliers over those made by foreign suppliers.

D. *Safeguards for Personal Information and Network Information Security*

— *Rules for Protecting Personal Information*

The CCL defines "personal information" as any information, recorded electronically or through other means, that, taken alone or together with other information, is sufficient to identify a natural person's identity, including, but not limited to, natural persons' full names, birth dates, identification numbers, personal biometric information, addresses and telephone numbers. Section 4 of the CCL stipulates rules that network operators must follow with respect to the protection of network users' personal information, including:

- Making public their rules for the collection and use of personal data;
- Explicitly stating the purposes and scope for such collection and use;
- Obtaining user consent for the collection and use of personal data;
- Not disclosing to any third party such personal information without the consent of the subject of such personal information;
- Providing individuals with the right to require that the network operator delete their personal information if an individual finds that the network operator has collected or used his or her personal information in violation of China's laws or in violation of an agreement between the user and the operator; and
- Providing individuals with the right to require that the network operator correct an error in their personal information if such information contains an error.

In addition, no person may obtain personal information through illegal means or sell or provide to others any personal information in violation of Chinese law. The Draft Data Transfer Measures, discussed below, contain additional measures to protect overseas transfer of personal data.

— *Rules for Ensuring Network Information Security*

Section 49 of the CCL stipulates rules that network operators must follow to ensure network information security, including:

- Establishing network information security complaint and reporting systems;
- Making complaints and self-assessment reports related to network information security publicly available; and
- Timely addressing such complaints and reports.

Additionally, the CCL obligates network operators to manage the information published and transmitted by its users, take measures to stop the transmission or distribution of, and eliminate, any illegal or prohibited information and report any prohibited incident to relevant governmental agencies. This means that network operators will need to monitor their online forums and perform audits of other areas where users can publish information.

— *Impact*

The CCL's safeguards for personal information and network information security represent a vast enhancement over existing Chinese laws. The CCL is the first Chinese law that comprehensively defines "personal information" and systematically regulates the collection and storage of personal information. In addition, it expands on citizens' rights with respect to their personal information and imposes more significant penalties for breach of protection of personal information. Network operators should note that the CCL does not delineate what constitutes sufficient user consent when collecting personal data—for example, whether an acknowledgement of policy with an option to opt-out is sufficient or whether a user must affirmatively opt in to the collection and use of their information. Pending clarification of what form of consent is required, network operators may choose to adopt a conservative

posture and obtain user consent by opt-in mechanisms pursuant to a written policy. Such an approach would likely be helpful in the event of a dispute as to whether the network operator obtained sufficient consent. For some global enterprises, the CCL's requirements may not be onerous, as such enterprises may already be implementing the foregoing practices in order to comply with laws in the EU and other jurisdictions.

E. *Requirements for Local Data Storage and Data Transfers*

— *Initial Scope of the Law*

Article 37 of the CCL requires that all personal information and "other important data" gathered or produced by an operator of critical information infrastructure in China must be stored in China. In addition, all outbound transfers of such information or data (which must be necessitated by business needs) will be subject to a security assessment conducted by the relevant departments of the State Council in accordance with the rules promulgated by such departments.

— *Expansion of the Law*

The Draft Data Transfer Measures, issued on April 11, 2017 and closed for public comment as of May 11, 2017, have the stated purpose of implementing Article 37. In fact, the Measures appear to expand the scope of Article 37 by setting forth requirements for local data storage and cross-border data transfer that apply to any network operator rather than just to operators of critical information infrastructure. No explanation for the apparent expansion of scope is provided. This broadened scope is expected to be an area of substantial pushback in public comments. The specific requirements, as set forth in the Draft Data Transfer Measures, are discussed below.

The Draft CII Regulations further expand the scope of Article 37 of the CCL by requiring (in Article 34) that the operation and maintenance of critical information infrastructure be carried out in the People's Republic of China ("PRC") and any remote maintenance from overseas that is necessitated by business needs be reported to the relevant industry regulators or PSB prior to such remote maintenance being conducted.

— *Consent for Transfer of Personal Information*

Under Article 4, all cross-border transfers of personal information require the consent of the person who is the subject of such information (or if such person is a minor, the consent of his or her guardian), after such person is informed of the purpose of the transfer, the scope, content and recipient of the transferred information and the country or region in which the recipient is located.

— *Network Operator Self-Assessment*

Under Article 7, each network operator is required to conduct a security self-assessment before making a cross-border data transfer.[7] Such self-assessment is subject to periodic inspections by the regulatory authorities of the industry in which the network operator operates. Each network operator must conduct at least one self-assessment each year and must report the outcome of such self-assessments to the competent industry regulators. In the case of any change in circumstances, such as a change of the data recipient or a change in the purpose, scope, amount or type of data transferred offshore, or any material data incident involving the data recipient or the data to be transferred, the security assessment must be promptly repeated.

— *Regulatory Assessment*

In addition to the requirements described above, the following cross-border data transfers will also be

[7] According to Article 8, a security assessment (including self-assessment) should focus on the following areas: necessity of data export; amount, scope, type and sensitivity of the personal information involved and whether the subject of the personal information has consented to such data export; amount, scope, type and sensitivity of any important data involved; security protection measures and capability of the data recipient, and the general environment for network security in the recipient country/region; risk of leak, destruction, abuse and tampering after data export; and risk to national security, public interest and personal rights imposed by data export and accumulation of data overseas.

subject to a security assessment by the relevant industry regulators, which must be completed within sixty (60) business days from the date of request for transfer (Article 9):

- Transfers (individually or in the aggregate) of personal information of over 500,000 Chinese citizens;
- Transfers exceeding 1,000 gigabytes;
- Transfers involving data regarding "nuclear facilities, chemical biology, national defense or military, population and health care, etc.," and data related to "large-scale engineering activities, marine environment, and sensitive geographic information";
- Transfers involving data related to cybersecurity information of China's critical information infrastructure operators, such as their system vulnerabilities or security measures;
- Transfers involving the provision of personal information and important data to overseas recipients by operators of critical information infrastructure; and
- Other transfers that the relevant industry regulator deems necessary to be subject to security assessment because they may potentially affect China's national security and public interests.

— *Prohibited Transfers*

The following cross-border data transfers are prohibited:

- Any transfer of personal information that has not been consented to by the subject of such information or that may impair the personal rights and interests of the subject of such information;
- Any transfer that poses a risk to China's national security or public interest; and
- Any transfer that is deemed by the Chinese government to be prohibited.

— *Penalties*

Article 46 of the Draft CII Regulations provides that any business that violates the in-country storage requirement or restrictions on outbound transfer of data is punishable by fines of ¥5,000 (~$725; ~€650) to ¥500,000 (~$72,500; ~€65,100), suspension of the related business, shutdown of the website or revocation of the related business license.

— *Impact*

The in-country data storage requirement and the restrictions on outbound transfers of personal information and other types of data, as well as the requirement to conduct maintenance of critical information infrastructure in the PRC, could pose disproportionate burdens on companies with global operations. The U.S. government affirmed such concern in a filing at the World Trade Organization, stating: "The impact of the measures would fall disproportionately on foreign service suppliers operating in China, as these suppliers must routinely transfer data back to headquarters and other affiliates. Companies located outside of China supplying services on a cross-border basis would be severely affected, as they must depend on access to data from their customers in China."[8] As alluded to in the U.S.'s statement, it is not clear how cloud-based service providers and global enterprises that require more flexibility in offshore data backup or remote management and maintenance are expected to work within these restrictions. The open-ended standard for types of information that might be prohibited or restricted in cross-border transfers provides a basis for the government to restrict a broad range of data if it so chooses. Finally, the CCL has not identified what form of consent would meet the requirement to obtain a person's consent for the cross-border transfers of personal information. Thus, covered entities should consider a conservative approach with respect to

[8] https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=238967,235083,234683,234548,233628,233629,232625,229594,229263,228945&CurrentCatalogueIdIndex=0&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=False

obtaining such consents and monitor CCL- and privacy-related case law, as it may provide future insight as to what constitutes sufficient user consent.

F. *Regulation of Internet News Information Services*

The Information Services Measures, effective as of June 1, 2017, require providers of internet news information services (including editing, publication, distribution and broadcast platform services for internet news) to obtain an internet news information service license. This requirement applies to all types of providers, including operators of websites, apps, forums, blogs, microblogs, public accounts, instant messaging tools, webcasts and any other form of digital communication.

The Information Services Measures also stipulate that a domestic business that wishes to set up a joint venture in this field with a foreign partner, or accept foreign funding, must be assessed by the State Internet Information Office. This could significantly impact joint ventures in a broad range of areas. Violation of this provision may result in a fine between ¥5,000 (~$725; ~€650) and ¥30,000 (~$4,400; ~€3,900). However, it is unclear if this provision applies to the onshore entity in a variable interest entity, or VIE, structure. Such structure is commonly used by foreign investors to address ownership limitations in restricted sectors, such as internet services in China.

G. *Penalties for Violation*

A majority of the violations of the CCL are only punishable by a fine between ¥5,000 (~$725; ~€650) and ¥1,000,000 (~$145,000; ~€130,000). The relatively minor penalties in most cases also raise questions as to the deterring effect of the CCL. Nonetheless, there are non-pecuniary penalties that are notable. The following violations may result in revocation of an entity's business or internet service license: (1) significant failure to collect authentic identification information from users or the provision of services to users that have not provided their authentic identification information; (2) violation of certain provisions relating to personal information protection; and (3) storage of data outside of China or transfer of data or information out of China in violation of the requirements in Article 37 for operators of critical information infrastructure. Persons engaging or assisting in cyber-attacks, theft of network data or other activities endangering network security and persons conducting criminal activities via networks may be detained for up to fifteen (15) days. Violations of the CCL can also be included in the credit history of the violating entity and be made public.

III. Key Takeaways

While the CCL marks a notable development in China's cybersecurity legislation, its lack of specificity in many areas means that many questions remain to be answered and implementation details remain to be addressed by future rulemaking. As discussed above, we anticipate further clarification to be provided in several areas, notably: the tiered system for compliance, critical network equipment and specialized network products, critical information infrastructure, data storage and data transfer and the procurement of network products and services.

Given the short implementation history of the CCL, its impact is not yet fully known, but it is foreseeable that the CCL and its related regulations will increase compliance costs for companies operating in China. For example, obtaining a safety certification for critical network equipment and specialized network security products, conducting maintenance of critical information infrastructure, ensuring certain data is stored in the PRC, satisfying a security assessment for certain cross-border transfers of personal information and managing access to online forums may be new obligations for some foreign companies; and it remains to be seen whether these and other obligations may have a disproportionate impact (or impose a disproportionate burden) on foreign companies as compared to local PRC companies.

Directors and management of companies operating in China should work closely with information technology officers and staff to examine existing policies and practices with a view to enhancing

preparedness and compliance. If companies are unsure whether they are subject to certain requirements, it may be advisable to consult with counsel. Companies should also monitor CCL developments as future rulemaking may provide additional clarity on the scope and specific requirements of the CCL.

From a policy perspective, the CCL reflects a growing global trend of nations and nation-states using legislative measures to promote the protection of personal information and cybersecurity. The New York Department of Financial Service's cybersecurity regulations[9] and the European Union's General Data Protection Regime and Network and Information Security Directive[10] are other examples of such laws and regulations. While these measures underscore that cybersecurity threats know no borders, they also raise concerns about the growing discrepancies between different jurisdictions in this area and the challenges that these discrepancies pose to multinational corporations in the digital era.

…

CLEARY GOTTLIEB

[9] https://www.clearygottlieb.com/news-and-insights/publication-listing/nydfs-cybersecurity-regulations-take-effect-8-21-17.
[10] https://www.clearygottlieb.com/news-and-insights/publication-listing/cybersecurity-in-the-eu-the-new-regime-under-the-gdpr-and-nisd-5-5-17.