Cybersecurity and Data Protection: A Study on China's New Cybersecurity Legal Regime and How It Affects Inbound Investment in China

Chen Ji

Recommended Citation
https://scholar.smu.edu/til/vol51/iss3/6

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in International Lawyer by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
Cybersecurity and Data Protection: A Study on China’s New Cybersecurity Legal Regime and How It Affects Inbound Investment in China

CHEN JI

I. Introduction

“Data is the lifeblood of the modern global economy. Digital trade and cross-border data flows are expected to continue to grow faster than the overall rate of global trade. Businesses use data to create value and many can only maximize that value when data can flow freely across borders.”

China’s highest legislative body issued its first cybersecurity law on November 7, 2016, which became effective nationwide on June 1, 2017 (“Cybersecurity Law”). Commentators opine that “businesses operating in China should [pay significant attention to the Cybersecurity Law] because it contains several provisions that could greatly impact their information security practices and liabilities.”

To date, the Chinese governments have issued several implementation rules to provide more detailed guidance on the general requirements set out in the Cybersecurity Law. Some of these implementation rules are in draft forms issued for public comments. Certain draft industry standards, once officially adopted, are voluntary only (meaning enterprises can choose whether to comply with such standards or not). However, this article still considers such voluntary standards because they provide detailed instructions to the general mandatory obligations. These voluntary standards may also serve as safe harbor in reality during governmental enforcement actions.

5. Id. para. 2.
6. Id. para. 24.
7. Id.
8. Id.
A spokesman of the Cyberspace Administration of China ("CAC") also held press conference on June 1, 2017 to respond to enterprise concerns and public questions on the Cybersecurity Law ("June 2017 Press Conference").

Comparing with the usual timeline that China passes its new laws, Chinese governments acted quickly in passing the new regime, showing China's determination in regulating its cyberspace.

Before issuance of the Cybersecurity Law, China already has an existing legal regime governing its cyberspace. However, such existing legal regime is generally regarded as relying only on lower-level legislation, piecemeal and not very well coordinated. The Cybersecurity Law is the first systematic approach at the highest legislative level for the Chinese governments to regulate its cyberspace. While enhancing protection set out under the existing legal regime, the new cybersecurity legal regime introduced new requirements (to be discussed below).

As a road map, Section 2 of this article outlines the basic framework of the new cybersecurity legal regime. Sections 3-5 respectively analyses the following “controversial” requirements introduced under the new regime and their impact on foreign investments in China: (1) data localization and cross-border transfer restrictions, (2) restrictions for network operators to collect and use personal data in China, and (3) PRC national cybersecurity review. Section 6 summarizes generally legal penalties for any violation of each of such obligations for completeness. Section 7 concludes with overall suggestions to foreign investors and legal advisors for evaluating investment in China.

Where applicable, this article compares the new Chinese cybersecurity legal regime against the relevant legal regime of the United States ("US"). I have particularly selected the US legal regime for comparison because the US appears to be the “toughest” contestor against the Cybersecurity Law.

Also, the US legal regime is one of the legal frameworks that the Chinese
governments mentioned to have studied in particular before issuing the new Chinese regime. This article also slightly discusses the legal regime of other countries/regions such as the European Union ("EU") to provide additional international context.

II. Overview on the Latest Chinese Cybersecurity Legal Regime

According to the CAC spokesman, the Cybersecurity Law is primarily enacted to protect national cybersecurity and the legal interests of enterprises and Chinese citizens. In responding to concerns from foreign enterprises, the spokesman responded that the law is not enacted to impede foreign enterprises, technology or products from accessing the Chinese market or to restrict legal cross-border data transfer.

The underlying rationale of the Cybersecurity Law is to divide the cyberspace into four parts and regulate each accordingly. These parts include: (1) the critical information infrastructure ("CII"), as the basic foundation, (2) above that, the intermediate Internet platforms (e.g., the e-commerce platforms), (3) further above, the Internet users, and (4) at the very top, the cyber-data of the Internet users. The Cybersecurity Law is one of the foundational cyberspace legislation designated to regulate CII operators and operators of other network facilities. The other foundational legislation being deliberated is the Telecommunication Law of the PRC whose goal is primarily to regulate data transmission issues.

The Cybersecurity Law governs any individual or entity that "construct, operate, maintain or use any 'network' within China and the overall cybersecurity in China". The definition of "network" and "network operators" are drafted broadly, and can cover telecommunication service providers such as Baidu, Alibaba, Tencent and potentially all businesses operating in China since nearly all businesses administer computer networks (a type of captured network) at least for internal use.

"Network operators" are further divided into the CII operator and other network operators with the CII operators subject to enhanced security
requirements. Other network operators are voluntary to comply with such enhanced requirements.

The Cybersecurity Law defines CII by two conjunctive parameters: any damage to or data leakage of a CII needs to possibly cause seriously harm to China’s national security (impact parameter), and (2) such infrastructure is utilized within certain key industries designated by the Chinese governments (industry parameter). The PRC State Council has the authority to issue and update specific scope of CII from time to time. Commentators have criticized such non-exclusive approach to define CII as providing “considerable leeway to bring industries not specifically singled out in the definition into [regulation] at a later stage”. However, it seems such approach is not uncommon as the US adopts a similar approach for the regulation of CII within its territory region, defining CII based on both the industry and impact parameters and giving authority to the Department of Homeland Security (“DHS”) to update the regulated scope from time to time.

Under published sources, CII in China is further narrowed down to any infrastructure of “network facilities, information systems, and/or Internet application systems” meeting the two parameters. Further, a seemingly internal governmental document provides additional guidance on CII identification. For example, the document identifies CII as “information systems or industry control systems” that can generally be classified into three categories: (1) websites (e.g., news media), (2) platforms (e.g., e-commerce platforms), and (3) manufacturing and business facilities (e.g., cloud centers). This document also outlines additional quantitative

27. See Wánglù wānjīn Fá, supra note 23, art. 31.
28. Id.
29. Id.
30. Gabriela Kennedy, Xiaoyan Zhang, China Passes Cybersecurity Law, MAYER BROWN JSM (Nov. 10, 2016), para. 2, https://www.mayerbrown.com/files/Publication/3c8214cb-f3a4-42c8-bc17-bb2f2749a03f/Presentation/PublicAttachment/c1a1df2-9d57-40bb-8a83-c5b518902c82/161110-HKGPCC-CybersecurityDataPrivacy-TMT.pdf.
parameters for identifying CII within each category and proposes specific steps to identify CII.

Applying the guidelines set out above, many CII will be managed by private enterprises. The CAC spokesman explained that this is also the case in the US where around eighty-seven percent of CII are managed by private enterprises.34

The Cybersecurity Law designates the CAC to be the authority coordinating efforts among all the other Chinese governments in regulating network operators. Other enforcement authorities include the Ministry of Industry and Information Technology, Ministry of Public Security, other industry regulators, and local governments.35 The US has a similar regulatory structure where the DHS is the overall authority coordinating all efforts among other federal and state governments in regulating CII.36

III. Data Localization / Cross-Border Transfer Restrictions

Before issuance of the new regime, there are existing legal requirements within specific industries (e.g., banking) on data localization and cross-border transfer restrictions.37 Such requirements are scattered in lower-level legislation and are limited to application within the specific industries.38 The Cybersecurity Law took the approach to generally regulate data storage and cross-border transfer nationwide.39

Under the Cybersecurity Law:

CII operators [1] should, store within China, any personal data [3] and important data [4] they have collected and/or produced during their operations in China [2]. If any CII operator needs to transfer [5] such data overseas for business reasons, the applicable security assessment [6] should be completed. .40

[1] Whose obligation? The Cybersecurity Law makes data localization and cross-border transfer restrictions an obligation only for CII operators.41

34. See Brunner & Suter, supra note 31.
35. See id. at arts. 8, 32.
36. See id. at 434.
38. See Jihong, supra note 11.
40. See WANGLUO ANQUAN FA, supra note 23 art. 37.
41. Jihong, supra note 11.
The CAC spokesman emphasized the same intention in the June 2017 Press Conference. However, two subsequent draft implementation rules have expanded such requirements to “any network operator.” The actual intention remains to be clarified.

[2] “Operations in China”: The Cybersecurity Law left this concept undefined. One draft implementation rule defines the concept as “doing business or providing products or services in China” (regardless of an entity’s incorporation jurisdiction). Doing business in China can be indicated through “using Chinese language in the business, using Renminbi as the settlement currency, or delivering products into the Chinese territory”. The last factor of “delivering products into China” can indicate the exterritorial effect of this rule.

However, if an entity is only providing products or services to foreign entities or foreign individuals and such business transaction does not involve “personal data” of Chinese citizens or any “important data”, such entity will not be considered as operating in China.46

[3] “Personal data” refers to:

Any type of information, recorded in electronic or other forms, which can be used, independently or in combination with other information, to identify a natural person’s personal identity, including a natural person’s name, date of birth, identity certificate number, biology-identified personal data [e.g., iris, fingerprint], address, telephone number, etc.47

To the extent any information has been technically processed so that it no longer identifies a certain natural person (and such disconnection is not recoverable), such information no longer qualifies as personal data.

---


43. See Information Security Technology Guidelines, art. 3.2, supra note 42.

44. Id.


46. See Information Security Technology Guidelines, art. 3.2, supra note 42.

47. See WANGLUO ANQIAN FA, supra note 23, art. 76-5; see also Information Security Technology Guidelines, art. 3.3, supra note 42.
data’ and are thus carved-out from the cross-border transfer restrictions.48

Based on such definition, “personal data” includes information of “natural person” only and not include information that identifies entities.

Originally, the draft version of the Cybersecurity Law limited the scope to be “personal data of Chinese citizens” as opposed to the seemingly border wording of any “personal data”.49 Whether the intention of such wording change is to extend protection to personal data of “foreign individuals” remains to be clarified.

The carve-out for technically processed information is favorable for enterprises to utilize data within the current big data era.

[4] “Important data”: The Cybersecurity Law left this concept undefined. One draft implementation rule defines it as:

Any data (including original data and derivative data) collected or produced by entities and individuals in China that closely relates to PRC national security, economic development, and public interest.

Any information that has been legally published through governmental channels ceases to be recognized as 'important data'.50

In addition to such general definition, the draft rule also provides illustrative examples of “important data” within twenty-seven industries (list not intended to be exclusive and can be updated by applicable regulatory authority from time to time).51 For example, “online e-commerce transaction records” and “habits and inclination of individual customers” are identified as “important data” within the e-commerce industry.52 “Technical plan, computer software, source code, database, technical report, and testing data” of a financial institution are identified as “important data” within the financial industry.53 Based on such broad identification, a large number of corporate business data could potentially be considered as “important data” and thus be subject to the restrictions.

[5] “Cross-border data transfer”: The Cybersecurity Law left this concept undefined. One draft implementation rule defines the concept broadly and the key factors are whether any non-PRC party is accessing the data and the location of such party when he/she reviews the data.54 As such, if a party were to access the data stored in China in New York, this can qualify as a transfer.55 If a foreign national reviews data physically in China, this may also qualify as a transfer. However, pure transmission of foreign data not

49. See Xiao, supra note 26, at 3.
50. See Information Security Technology Guidelines, art. 3.5, supra note 42.
51. Id. Exhibit A.
52. Id. Exhibit A 26-c.
53. Id. Exhibit A 19.1-b.
54. Id. art. 3.7

PUBLISHED IN COOPERATION WITH
SMU DEDMAN SCHOOL OF LAW
involving any local data produced as part of “operations in China” is carved out from complying with the restrictions. In such case, China is being used as a pure intermediary for processing or transmitting foreign data.56

[6] Security assessment: Security assessment is generally divided into self-evaluation or governmental evaluation.57 To the extent that a governmental evaluation is not triggered, an entity should conduct self-evaluation and file the evaluation report with the applicable Chinese government.58

Any security assessment is generally a two-step process. An entity first assesses the “legality, rightfulness and necessity” for the cross-border data transfer.59 Once a transfer is concluded as legal, rightful and necessary, a second step is to assess the overall security risk for the transfer.60 There are specific parameters as to how evaluation should be conducted during each step.

Based on the outlined parameters, there are four possible evaluation results – transfer risk identified as either low, medium, high or extremely high. An entity is allowed to proceed with the cross-border data transfer if the transfer risk is identified as low or medium. However, if the evaluation result is either high or extremely high, the transfer is prohibited.61 An entity is allowed to take on additional risk mitigation methods (e.g., reduce the amount of data to be exported) to lower the risk and conduct re-evaluation.62 If there is any material change to the evaluated information (change to data recipient presumed material) after completion of a transfer, an entity should complete security assessment again via the same process.63

[7] Other considerations:

(a) Consents by an individual to transfer his/her “personal data”: There is some ambiguity as to whether an individual’s consent can exempt an entity entirely from security assessment, or if consent will only establish legality of the transfer, and other parameters of a security assessment should still be evaluated. The CAC spokesman seems to support the former,64 while a draft implementation rule appears to take the latter approach.65

In any event, an entity must generally obtain consent from the applicable individuals before transferring his/her “personal data”. Consent must be expressly given (e.g., through an online opt-in mechanism) or implied through active behaviors (e.g., an individual voluntarily initiates cross-border online shopping disclosing his/her personal data).66 Before obtaining

56. Id. art. 3.7.
57. See Information Security Technology Guidelines, arts. 7, 9, supra note 42.
58. Id. art. 7.
59. Id. art. 5.1.
60. Id. arts. 4.2.1, 4.3.1.
61. Id. art 4.2.5.
62. Id. arts. 4.2.5, 4.2.7.
63. See Information Security Technology Guidelines, art. 12, supra note 42.
64. See Hang, supra note 9.
65. See Information Security Technology Guidelines, art. 5.1a, supra note 42.
66. Id. art 3.2.
consent, the entity transferring the data should inform the individual of certain important information that a data subject should know for giving the consent (e.g., the data recipient). Any material change to such information warrants a new consent from the relevant individuals (change to recipients of the data presumed material).

(b) International agreements entered into by China on cross-border data transfer: a draft implementation rule provides a potential outlet for complying with the security assessment regime. That is, any specific cross-border data transfer arrangement entered into by China with international organizations or foreign countries may preempt requirements under the Cybersecurity Law. To date, I am not aware of any special international agreements China has entered into in such respect. A CAC representative has expressed that this outlet might be a future channel to initiate international dialog or bargain on the cross-border data transfer issues.

General comments: Requesting data localization and imposing cross-border transfer restrictions is not uncommon internationally. Starting from legislation in the EU, more than sixty-nine nations internationally have enacted such restrictions, including Canada, Australia, etc. Further, commentators opine that regulations on data localization and cross-border transfer are legitimate under the WTO GATS rules due to the “general exception” thereunder permitting member countries to adopt legislation “protecting personal privacy in data processing and dissemination and confidentiality of personal records and accounts.”

But any overly restricted cross-border data transfer requirements could harm the interests of business enterprises and eventually harm the enacting nation by isolating such nation from the rest of the world. As such, scholars in China have emphasized the need to balance data protection and business needs of global enterprises. Fortunately, major market players in China such as Alibaba and Tencent have been involved in designing the cross-border data transfer guidelines and hopefully will make their voice heard during the legislative process.

In comparison, US companies (such as IBM) have long been recognized as possessing the highest capability in processing data within a cross-border context and have significantly benefited from the international flow of

67. Id. art. 5.1.
68. Id.
69. Id. art 15.
72. See id.
73. Zhonglun Cybersecurity Law Interpretation, supra note 11.
74. Id.
Within such context, the US generally favors free flow of information and opposes the imposition of cross-border transfer restrictions. Against such background, there are few express restrictions on storing personal data outside the US, but some states have restrictions on data access, maintenance, and processing from outside the US with respect to government contracts and offshore outsourcing situations. Some federal agencies can also impose such restrictions in their contracts. Otherwise, a requirement to store personal data in the US usually manifests as a contractual requirement where a customer is apprehensive about sensitive data being stored in jurisdictions which are perceived as having a weak personal data protection regime.

Impact on foreign investment in China: When evaluating a Chinese target, foreign investors may consider conducting due diligence on applicability of any Chinese data localization and cross-border transfer restrictions. To the extent the target is subject to any such requirements, a foreign investor can factor any cost required for compliance (e.g., ongoing cost that may be required to maintain a separate data server in China) into the purchase price and ongoing business plans.

Within the international dispute resolution context, foreign investors may wish to engage an e-discovery specialist at the earliest stage to analyze the feasibility and timing required to transfer any evidence stored in China. Having said that, as certain Chinese requirements may not be entirely clear, whether to transfer certain data outside of China or not might eventually be a balancing test as to the actual non-compliance risk. On the other hand, absent any negative legal inferences against the party which fails to provide the requested data, any cross-border transfer restriction might work to a party’s benefit (e.g., serving as a justified defense in not submitting certain data to the dispute resolution tribunal).

IV. Restrictions on Collecting and Using “Personal Data”

The Cybersecurity Law does not substantially change the existing Chinese legal regime with respect to the collection and use of “personal data” in

76. Id.
78. Id.
79. Id.
81. Akerman et al., supra note 55, at 393 (discussing cross-border transfer restrictions will make US judges and private enterprises do a balancing test of required discovery materials).
82. Id. at 394 (discussing the cross-border transfer requirements can work both ways, sometimes can harm but sometimes may be helpful).
China. The key to ensure compliance is obtaining users’ consent regarding any collection, use, or other disposal of any personal data. But among others, the Cybersecurity Law does introduce two new interesting requirements, as discussed below.

Security breach notification law: Before issuance of the Cybersecurity Law, there was no nationwide requirement for notifying data subjects of a data security breach (such requirement might be available in certain local districts, e.g., in Shanghai). The Cybersecurity Law makes such security breach notification a nationwide obligation. Considering the substantial cost that might be incurred for compliance, commentators opine that such obligation will serve as a deterrent such that network operators will carefully safeguard the data to avoid any notification. In a recent case, Uber failed to notify around fifty-seven million users about Uber’s information leakage incident, resulting in a governmental investigation. Uber’s case shows the potential vast liability and cost associated with a security breach notification. As of April 2017, forty-eight of the United States, as well as the District of Columbia, Puerto Rico and the US Virgin Islands have all enacted laws requiring notification of security breaches involving personal data. Alabama and South Dakota are the only states without a security breach law.

The Cybersecurity Law requires “timely” notification to data subjects, but what this means remains to be clarified. In comparison, the typical standard in the US (set out under various state laws) is notification to data subjects within thirty days without unreasonable delay.

Right to be forgotten: The right to be forgotten (which took root in the EU) is newly enacted under PRC laws, overruling an earlier 2016 Beijing case which held that there is no right to be forgotten under Chinese laws.

---

83. Zhonglun Cybersecurity Law Interpretation, supra note 11.
88. Id.
89. Ackerman et al., supra note 55, at 410.k, Joanna, David, 2016 Cross-Border Panel Discussion, supra note 55, at 410.
90. See Ling, supra note 85.
In that case, Chinese courts in Beijing ruled in favor of Baidu in a lawsuit over removing search results of Ren Jiayu. It was the first of such cases to be heard in Chinese courts. In the suit, Ren Jiayu sued the Chinese search engine Baidu over search results that associated him with a previous employer. The courts ruled against Ren, and held, among other things, that there is no “right of forgotten” enacted under PRC laws so no relief can be granted.

This case shows how the new right to be forgotten may potentially affect court rulings and create potential costs for network operators in satisfying requests from individual users to delete their personal data.

In comparison, data subjects in the US currently have no right to request the deletion of their data under applicable federal laws. Under the Health Insurance Portability and Accountability Act ("HIPAA"), an individual can request inaccurate or incomplete information be amended. But the entity covered under HIPAA is not required to amend the data. As for state laws, the California Online Privacy Protection Act requires operators of web sites, online services, and mobile apps that are directed to minors—or that have actual knowledge that a minor is using their site or service—to permit a minor (as a registered user) to remove or request the removal of certain online information that she/he posted. The law does not apply to content for which the minor “received compensation or other consideration.”

Impact on foreign investment in China: A potential foreign investor should review existing business practice in China against compliance and factor any cost required for ongoing compliance into the purchase price and future business plans.

V. National Cybersecurity Review

Under the Cybersecurity Law, if the purchase by CII operators of network products and services may affect national security, CII operators should complete national cybersecurity review organized by Chinese governments.
(essentially a supply-chain review). It is expected that the applicable industry regulators will further issue catalogs to identify the specific vendor products and services subject to the cybersecurity review.

The available security review requirements and the structure of the proposed review authority are general brush strokes and remain to be further clarified (e.g., how to review early manufacturing and/or testing stages of the vendor products, whether foreign shareholding background of the vendors should be considered, etc.).

Foreign companies have raised concerns that the national cybersecurity review process is a disguise of local protectionism (i.e., to screen out foreign products and services). The CAC spokesman countered that the review does not target to exclude or discriminate against products or services from particular regions and is not intended to restrict the Chinese market from foreign products or services. According to the spokesman, the goal for implementing the cybersecurity review is to boost consumer confidence and increase market potentials for all businesses.

In the US, security review on supply-chain is not uncommon when the utilization of cyber products or services has national security implications. For example, in November 2013, the Department of Defense issued interim rules requiring supply-chain review with respect to procurements related to national security systems ("NSS"). Information systems need not be used or operated by a government agency in order to qualify as NSS's. There


104. See Hang, supra note 9.

105. Id.


are also similar supply-chain security review requirements for cloud service providers under the Federal Risk and Authorization Management Program.108

Comparison with Foreign Investment National Security Review: The Chinese foreign investment national security review (Chinese counterpart of the US CFIUS review) is separate and different from the cybersecurity review discussed above.

The foreign investment review is a mandatory process applying to foreign investment (taking control) in Chinese companies that has national security implications.109 National security implications can generally be indicated by foreign investment into sensitive industries (e.g., military products, critical infrastructure, etc.), or foreign investment into enterprises located nearby major and sensitive military facilities.110 Control does not necessarily refer to possessing more than fifty percent shareholding interests in the target Chinese company, and can cover any scenario where a foreign investor controls the business, decision-making, financial, or technology of a China target.111

A special committee consisting of representatives of various Chinese governments (commerce departments, reform and development departments, etc.) organizes the foreign investment review.112 Upon review, if the special committee deems that a transaction may impact PRC national security, the committee has blocking rights or can order divestiture of particular assets even after a transaction is closed.113

Impact on foreign investment in China: Be aware that there are two types of different PRC national security review. Factor any applicable security review requirements into project timelines and ongoing business plans.

VI. Penalty for Violation of the Cybersecurity Law\textsuperscript{114}

Administrative penalties: Generally speaking, violation of the requirements set out under the Cybersecurity Law may subject an entity to administrative fines of up to USD $75,777, an order from the competent regulatory authority to cease business operation, possible confiscation of all illegally earned income, shut down of the relevant website, and/or revocation of the relevant business permit/license of the network operator, and a fine of up to RMB 100,000 (around USD $15,155) can be imposed on the directly responsible person in charge* and other liable persons** of the CII operator.\textsuperscript{115}

Civil right of action: Any violation of the Cybersecurity Law by a network operator entitles a private right of action against such network operator for civil liabilities.\textsuperscript{116}

Criminal liabilities: Violation of the Cybersecurity Law and certain of its implementation rules could warrant criminal liability for “failure to comply with cybersecurity management obligations” and “infringement on Chinese citizens’ personal data”.\textsuperscript{117} In either of such cases, an entity deemed to commit such a crime will be imposed with fines, and its directly responsible person in charge* and other directly liable persons** could be punished with life sentences.

*“Directly responsible person in charge refers to individuals who decides, approves, directs, or allows the violation by an entity, and normally includes the chief responsible person of an entity (including the legal representative of the entity).

**Other directly liable persons refer to individuals who implements the actual violation of an entity and plays significant role within the process. Such persons can include managers and employees of an entity.”\textsuperscript{118}

\textsuperscript{114.} RMB:USD calculated based on an exchange rate of 1 USD: 6.59830819 RMB, applicable as of November 26, 2017.

\textsuperscript{115.} See, e.g., Cybersecurity Law, supra note 23, art. 66.

\textsuperscript{116.} Id. art. 74.

\textsuperscript{117.} Zhonglun Cybersecurity Law Interpretation, supra note 11; see Dong Xiao, Liang Gao Jiebi Daizai Qye Xinxihuogu de Xinluozaoshan (两高解释带来企业信息合规的新挑战) [New Interpretation From SPC And SPP Provides New Compliance Challenges For Enterprises] JUNHE, (May 26, 2017), http://www.junhe.com/law-reviews/638 (last visited June 14, 2018).

“Legal representative” is a position that each company incorporated in China is required to have under PRC laws. A legal representative can generally take actions on behalf of a company which binds such company. Considering the potential personal liability of a legal representative in criminal violation context, foreign investors are suggested to carefully choose a legal representative candidate while balancing control over a China subsidiary.

VII. Conclusion

Traditionally, when a foreign investor evaluates a potential investment in China, Chinese cybersecurity and data protection requirements is not an area for due diligence. But with the issuance of the Cybersecurity Law and its implementation rules, the various requirements set out under such rules may impact the business and legal assumptions that foreign investors make regarding Chinese inbound investments.

As such, foreign investors may wish to review the Chinese cybersecurity legal regime as part of their due diligence and factor any identified issues into the purchase price, project timeline, and ongoing business models (as applicable). A foreign investor may also wish to engage a cross-border e-discovery expert at the earliest stage to coordinate global efforts in any international dispute resolution proceeding.

Eventually, it may boil down to a risk-based decision, as there may be some nuance in complying with every country’s laws and requirements (considering certain laws and regulations are themselves not clear and require judgments on compliance) while satisfying interests of each stakeholder within the corporate structure. Similarly, a legal counsel may need to provide a thought-through analysis weighing the risks of different factors (taking into account the relevant enforcement practice) to enable a corporate decision-maker to decide the proper way forward.

119. Ackerman et al., supra note 55, at 392 (discussing [a party is] never going to be able to comply with every country’s laws . . . and . . . make shareholders happy, and do all of those things that companies want to do).
120. Id. at 393.