WILMERHALE

Navigating China's Data Security Laws in US Discovery

April 3, 2024

The enactment of China's Cybersecurity Law (CSL),[1] Data Security Law (DSL),[2] and Personal Information Protection Law (PIPL, together with the CSL and the DSL, "Data Security Laws")[3] has significantly reshaped the landscape of data security and personal privacy for China, not just within its own borders but also in the context of cross-border data transfers. The broad scope and ambiguous language of these Data Security Laws, however, introduce a heightened level of complexity to the process of discovery in US litigation involving Chinese entities or individuals or other sensitive or personal data in China. This article explores the intricacies of these laws and accompanying regulations and rules and their implications for US litigants pursuing discovery from Chinese counterparts, as well as for Chinese entities and individuals who are subject to discovery requests in US federal litigation.

I. CHINA'S DATA SECURITY LAWS

CSL. As relevant here, the CSL requires "[c]ritical information infrastructure [CII] operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China [PRC]" to store such data within China.[4] "Where due to

[1] Stanford University, *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/. These citations to the translated versions are for reference only. As discussed below, statutory interpretation issues may arise when parties present different translations of the same statute.
[2] Stanford University, *Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2017)*, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/.
[3] Stanford University, *Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021)*, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/. The three Data Security Laws apply only to Mainland China; references to "China" in this article therefore refer to Mainland China.
[4] CSL, art. 37.

business requirements it is truly necessary to provide it outside the mainland," they must conduct a "security assessment."[5]

The CSL, along with the later promulgated CII Security Protection Regulations ("Security Protection Regulations"),[6] defines CII broadly to include infrastructure from a wide array of "important industries and sectors."[7] "Personal information" is likewise defined broadly under the CSL to include "all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity[.]"[8] While "important data" is undefined under either the CSL or the Security Protection Regulations, the Chinese government has recently clarified that "unless data processors are informed by relevant industry regulators or local governments that relevant data constitutes 'important data' or is defined as 'important data' in the published rules, data processors do not need to treat any data as 'important data' or conduct a data export security assessment."[9]

DSL. As relevant here, the DSL states that "[d]omestic organizations and individuals must not provide data stored within the mainland territory of the PRC to the justice or law enforcement institutions of foreign countries without the approval of the competent authorities of the PRC."[10] The term "competent authorit[y]" is left undefined. Under the DSL, "data" is defined broadly as "any information record in electronic or other form."[11]

PIPL. Similar to the DSL, the PIPL provides that "[w]ithout the approval of the competent authorities of the People's Republic of China, personal information handlers may not provide personal information stored within the mainland territory of the People's Republic of China to foreign judicial or law enforcement agencies."[12]

As a general matter, the PIPL applies to both domestic and extraterritorial processing of data. It applies to "the activities of handling the personal information of natural persons within [China]";[13] it also applies to "handling activities outside [China] of personal information of natural persons within [China]" if one of these three circumstances is met: (1) where the data processing is for the purpose of "provid[ing] products or services to natural persons inside the borders"; (2) where the processing is done for the purpose of "analyzing or assessing activities of natural persons inside the borders"; and (3) under "[o]ther circumstances provided in laws or any administrative

[5] *Id.*
[6] Stanford University, *Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021)*, https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/.
[7] Security Protection Regulations, art. 2; *see also* CSL, art. 31.
[8] CSL, art. 76(5).
[9] L. Ross, K. Zhou and T. Liu, *China Finalizes Rules to Ease Data Export Compliance Burden (March 26, 2024)*, https://www.wilmerhale.com/en/insights/client-alerts/20240326-china-finalizes-rules-to-ease-data-export-compliance-burden.
[10] DSL, art. 36.
[11] *Id.*, art. 3.
[12] PIPL, art. 41.
[13] PIPL, art. 3.

regulations."[14] Whether the processing is domestic or extraterritorial, a personal information processor can process personal information only if one of seven circumstances exists, of which the following are potentially relevant for the purpose of this article: (1) the individual's consent has been obtained; (2) the processing is "necessary to fulfill statutory duties and responsibilities or statutory obligations"; and (3) "[o]ther circumstances provided in laws and administrative regulations."[15]

Generally, a personal information processor that "truly need[s] to provide personal information outside [China] for business or other such requirements" must go through one of the following three procedures: (1) passing the security assessment on outbound data transfer organized by the Cyberspace Administration of China (CAC); (2) obtaining the personal information protection certification from an authorized certification institution; or (3) entering into a contract with the overseas recipient based on the standard contract announced by the CAC.[16]

Under the PIPL, "personal information," or "PI," is defined as "all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization handling."[17]

II. HOW US FEDERAL COURTS APPROACH DISCOVERY OBJECTIONS BASED ON CHINA'S DATA SECURITY LAWS

China has since then promulgated various regulations and rules to facilitate the construction and implementation of the three Data Security Laws.[18] Yet a critical question remains unanswered: To what extent do these Data Security Laws affect a Chinese party or non-party's compliance with the discovery obligation to produce documents in US federal litigation?

This uncertainty has posed challenges to litigants and courts in the United States, most often in federal litigation. In examining this issue, it is helpful to start with the fundamental analytical framework employed by US courts. When a Chinese party or non-party invokes China's Data Security Laws to oppose discovery requests or subpoenas in a US litigation for document production, courts conduct the same two-step analysis that applies to other foreign blocking

[14] *Id.*
[15] *Id.*, art. 13, §§ 1, 3, 7.
[16] *Id.*, art. 38.
[17] *Id.*, art. 4.
[18] *See, e.g.*, L. Ross, K. Zhou and T. Liu, *China Updates Specification on Security Certification for Cross-Border Personal Information Processing Activities (Jan. 4, 2023)*, https://www.wilmerhale.com/en/insights/client-alerts/20230104-china-updates-specification-on-security-certification-for-crossborder-personal-information-processing-activities; L. Ross, K. Zhou and T. Liu, *China Finalizes Rules to Ease Data Export Compliance Burden (Mar. 26, 2024)*, https://www.wilmerhale.com/en/insights/client-alerts/20240326-china-finalizes-rules-to-ease-data-export-compliance-burden.

statutes. First, the court assesses whether China's Data Security Laws in question actually bar the requested discovery. Second, if the answer to the first step is affirmative, the court proceeds with an "international comity" analysis—a multifactor analysis that involves balancing the respective interests of the United States and China—to determine whether to grant the production request despite enforcement difficulty.

A. Step 1: Whether the Data Security Laws Bar the Discovery at Issue

At the first step, the party challenging the discovery request bears the burden to persuade the court that the requested production would indeed be barred by the relevant Data Security Laws. To satisfy this burden, the challenging party must provide information of "sufficient particularity and specificity" to allow the court to make the determination.[19] While a "document-by-document log of the documents" that could potentially be subject to the restrictions may not be necessary, the challenging party should at least describe the "categories" of documents at issue.[20]

In addition, during the first step, the challenging party must also substantiate why the Data Security Laws apply to the documents at issue. While parties often rely on their respective expert opinions regarding the legislative intent and statutory interpretation, some courts have exhibited skepticism toward these expert opinions for various reasons. For example, one court noted that conflicting expert opinions lack utility in the absence of guidance from Chinese official authorities (e.g., a decision from a Chinese court).[21] Another court concluded that it need not rely on expert opinions, as the English versions of these laws are readily accessible online, allowing the court to engage in its own statutory interpretation.[22] And where conflicting translated versions were presented by parties' experts, a court may conduct its independent analysis before endorsing one expert's translation.[23] Alternatively, the challenging party may satisfy its burden by presenting interpretations by Chinese authorities of the relevant Data Security Laws, which courts appear more inclined to consider.[24] As discussed below, recent case law has presented some interesting statutory interpretation issues, particularly concerning the DSL and the PIPL.

[19] *Philips Med. Sys. (Cleveland), Inc. v. Buan*, 2022 WL 602485, at *5 (N.D. Ill. Mar. 1, 2022).
[20] *Owen v. Elastos Found.*, 343 F.R.D. 268, 283 (S.D.N.Y. Jan. 11, 2023).
[21] *Concepts NREC, LLC v. Qiu*, 662 F. Supp. 3d 496, 526 (D. Vt. 2023).
[22] *Philips*, 2022 WL 602485, at *3.
[23] *Cadence Design Sys., Inc. v. Syntronic AB*, 2022 WL 2290593, at *4 (N.D. Cal. June 24, 2022).
[24] *Motorola Sols. Inc. v. Hytera Comms. Corp. Ltd.*, 2023 WL 5956992, at *5 (N.D. Ill. Sept. 12, 2023) (interpreting the CSL); *Owen*, 343 F.R.D. at 285 (considering drafter's commentary).

1. Whether the Information Sought Constitutes Regulated Data

Due to the expansive definition of data or information under the Data Security Laws, it is unsurprising that disputes often arise regarding whether the information sought by discovery falls within the ambit of regulated data under the Data Security Laws.

For example, in *Owen v. Elastos Foundation*, the federal court in the Southern District of New York agreed with the challenging party that business emails and documents are subject to the PIPL because they contain "personal information."[25] The court reasoned that the PIPL separately defines a narrower category of information as "sensitive personal information" and that, by contrast, the terms "business documents" and "business communications" appear nowhere in the DSL, suggesting that they should not be excluded from the more expansive "personal information."[26] On the other hand, in *Concepts NREC, LLC v. Qiu*, where the challenging party invoked the DSL, the federal court in the District of Vermont expressed skepticism regarding the DSL's overbroad definition of "data," which, as the court noted, "potentially encompasses every conceivable form of recorded information."[27] Such an expansive definition, according to the court, "appears inconsistent with the free flow of data across borders, particularly in the context of international commercial transactions."[28] Because of this and other ambiguities discussed below, however, the court went on to conduct the comity analysis given "the potential application of the DSL as a 'blocking statute.'"[29]

Parties may also disagree about the law's geographic limitations on the data. As to both the DSL and the PIPL, only data stored within China falls under regulatory purview. But what about data stored within China that has been made available at some point outside China? At least one court held that the PIPL is ambiguous on this point and therefore requires the court to go to the next step—the comity analysis.[30]

2. Whether Producing Documents Constitutes Regulated Data Processing Activity

The other often litigated issue is whether the discovery process—processing and producing documents—counts as regulated conduct under the Data Security Laws.

For example, courts split on the issue of whether discovery constitutes "provid[ing] foreign judicial or law enforcement authorities with the data" of which approval from "competent authorities of the People's Republic of China" must be obtained in advance, language that appears in both the DSL and the PIPL. At least three different federal courts have held that this language is not triggered by producing documents in discovery because discovery consists of

[25] 343 F.R.D. at 284.
[26] *Id.*
[27] *Concepts NREC*, 662 F. Supp. 3d at 527–528.
[28] *Id.* at 528.
[29] *Id.* at 528–529.
[30] *Id.*

exchanging information between the parties, not providing information to the US courts.[31] One other court disagreed with this reading, noting that the statute is ambiguous on the issue of whether a production would become one made to a "foreign judicial authority" if it is made pursuant to a US court's order granting a motion to compel.[32]

Moreover, it remains unclear whether this approval procedure for disclosing data to foreign judicial or law enforcement authorities operates independently or can be substituted by one of the three abovementioned compliance measures that generally apply to data processing under the Data Security Laws (i.e., security assessment, personal information protection certification or standard contract). Regardless, both sides should carefully consider whether compliance with US discovery obligations also triggers other provisions of the Data Security Laws, thus requiring the data processor to go through one of the three compliance measures.

For instance, limited case law interpreting the PIPL suggests that processing and production of documents to comply with discovery obligations qualifies as "processing" personal information under the PIPL.[33] But this is not the end of inquiry. As mentioned above, the PIPL distinguishes data processing outside China and inside China. For processing outside China, such as collecting data stored on servers located outside China, the statute applies only if any of three enumerated circumstances applies, including, as relevant here, where the processing is done for the purpose of "analyzing or evaluating the behaviors of natural persons within the territory of the People's Republic of China" and under "any other circumstance as provided by any law or administrative regulation."[34] In *Owen*, the challenging party tried to invoke the PIPL through a somewhat creative argument—that the requesting party may use the documents to "understand the conduct of [responding party]'s custodians."[35] The court rejected this argument, relying on the PIPL drafter commentary cited by the requesting party's expert.[36] On the other hand, *Owen* suggests that for data processing inside China, the responding party will likely be able to invoke the PIPL—in particular, that the processing "is necessary for the performance of statutory duties or obligations" or under "other circumstances provided by laws or administrative regulations."[37] Notably, the *Owen* court appears to have overlooked that the same "other circumstances provided by laws or administrative regulations" language is among the three circumstances that would bring data processing outside China within the ambit of the PIPL.

[31] *See, e.g.*, *Motorola*, 2023 WL 5956992, at *5; *Philips Medical*, 2022 WL 602485, at *6; *In re Valsartan, Losartan, and Irbesartan Prods. Liab. Litig.*, 2021 WL 6010575, at *10 (D.N.J. Dec. 20, 2021).
[32] *Concepts NREC*, 662 F. Supp. 3d at 527.
[33] *Owen*, 343 F.R.D. at 284; *Cadence*, 2022 WL 2290593, at *5.
[34] *Supra*, Pt. I.
[35] *Owen*, 343 F.R.D. at 285.
[36] *Id.*
[37] *Id.* at 285–286; *see also Cadence*, 2022 WL 2290593, at *5.

B. Step 2: Comity Analysis

When a court determines that at least one Data Security Law potentially bars document production, it proceeds to conduct a multifactor comity analysis. Courts typically consider at least these five factors:

> (1) the importance to the investigation or litigation of the documents or other information requested; (2) the degree of specificity of the request; (3) whether the information originated in the United States; (4) the availability of alternative means of securing the information; and (5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine the important interests of the state where the information is located (e.g., China).[38]

Courts in other circuits also consider other factors. For example, the Ninth Circuit considers "the extent to which enforcement by action of either state can reasonably be expected to achieve compliance with the rule prescribed by that state."[39] The Ninth Circuit, along with courts in the Second Circuit, has also taken into account the hardship of compliance on the party or witness from whom discovery is sought.[40] Courts in the Second Circuit also factor in "the good faith of the party resisting discovery."[41] We discuss each of these factors below.

***Importance and specificity of the requested discovery*.** Courts usually have no issue finding these two factors favor production. This is especially so when the requested information is likely to be critical evidence in the case, such as source code or trade secrets allegedly misappropriated by a Chinese party or its non-party affiliates.[42]

Where the requested information originated. This is usually a highly contentious factor. For example, when a Chinese party faces accusations of misappropriating source code, one key issue in the case would be where the source code "originated."[43] Given the contentious nature of this issue, this factor tends to be neutral or slightly against production.

Availability of alternative means. Courts also encounter no difficulty in concluding that alternative means of securing the information are unavailable. This factor merely requires the requesting party to demonstrate that the information cannot be "easily obtained" through alternative means.[44] And this showing can be satisfied through multiple ways, for example, the nonviability of securing discovery in China through the Hague Convention or the

---

[38] *Societe Nationale Industrielle Aerospatiale v. U.S. District Court*, 482 U.S. 522, 544 n.28 (1987).
[39] *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468, 1475 (9th Cir. 1992).
[40] *Richmark*, 959 F.2d at 1475; *Owen*, 343 F.R.D. at 282.
[41] *Owen*, 343 F.R.D. at 282 (collecting district court cases in the Second Circuit).
[42] *Motorola*, 2023 WL 5956992, at *6.
[43] *Id.* at 287; *see also Motorola*, 2023 WL 5956992, at *7; *but see Concepts NREC*, 662 F. Supp. 3d at 530 (noting this factor "only addresses the physical location of the documents," while concluding this factor is neutral "[b]ecause the location of the information remains unclear").
[44] *Concepts NREC*, 662 F. Supp. 3d at 530–531.

overburdensome cost of seeking discovery through subpoenaing US-based service providers (e.g., subpoenaing a third-party server vendor for all the documents the challenging party stored on the server).[45]

Balance of the interests of China and the United States. This is the "most important" factor of the comity analysis,[46] often tilting in favor of enforcing the requested discovery. In intellectual property cases, courts have consistently prioritized the United States' interest in safeguarding intellectual property rights over China's data security concerns.[47] One court even cautioned that even if the responding party sought from Chinese authorities either permission to produce the information or guidance that the production would violate Chinese law, this alone does not necessarily compel a finding that Chinese interests outweigh those of the United States.[48]

Likelihood of compliance and hardship to Chinese litigant. These two factors likely favor complying with discovery requests. As explained above, courts in the United States will not likely construe the Data Security Laws to be a per se bar to document production. Likewise, courts usually have no trouble finding that the lack of information showing any "hardship of compliance" favors production. At least as of September 2023, there had been no evidence of a Chinese individual or company being penalized for the production of documents or data for use in discovery in US litigation.[49] On the other hand, "discovery and contempt orders [issued by a US court] may be of some significance" to a Chinese litigant that has assets, or wishes to continue with its business, in the United States.[50]

Good faith of party resisting discovery. In considering this factor, courts will likely closely scrutinize the resisting party's prior representations and conduct. For example, in *Motorola Solutions Inc. v. Hytera Communications Corporation Ltd.*, the federal court in the Northern District of Illinois found this factor against the Chinese company when it "waited until the eleventh hour to first raise *any* concern regarding the application of Chinese Data Security Laws" and failed to mention its pending request for permission from the Chinese government when promising to the requesting party that it would produce the source code.[51] As another example, the court in *Owen*, though "hav[ing] no reason to doubt the Chinese defendants' good faith in interposing PIPL as an objection," deemed this factor "neutral."[52] The court's conclusion was influenced by a number of inaccurate factual assertions made by the defendants, including whether some of the custodians were actually in China, and the finding

[45] *Owen*, 343 F.R.D. at 287.
[46] *Concepts NREC*, 662 F. Supp. 3d at 532.
[47] *See, e.g.*, *id.* at 531–532; *Philips Medical*, 2022 WL 602485, at *6; *Owen*, 343 F.R.D. at 288.
[48] *Concepts NREC*, 662 F. Supp. 3d at 532.
[49] *Motorola*, 2023 WL 5956992, at *9.
[50] *Richmark*, 959 F.2d at 1478.
[51] *Motorola*, 2023 WL 5956992, at *9 (emphasis in original).
[52] *Owen*, 343 F.R.D at 288–289.

that the defendants did not search all the relevant devices or accounts of those custodians who consented to the search.[53]

On balance, case law so far indicates that the comity analysis tends to favor the party seeking discovery from Chinese companies or individuals.

III. IMPLICATIONS AND RECOMMENDATIONS

All three Data Security Laws cover broad categories of information and contain various ambiguities open to interpretation. Absent formal guidance from Chinese authorities, and coupled with Chinese courts' general reluctance to order production of data in foreign judicial proceedings, the responsibility to navigate these murky waters squarely rests with US courts as they continue to grapple with discovery issues involving Chinese entities and individuals.

For parties seeking discovery from Chinese entities or individuals, thorough preparation is essential to counter the resisting party's statutory arguments in the first step—specifically how the Data Security Law(s) at issue might block the production. However, it is prudent to anticipate that the resisting party may prevail in the first step and to focus on substantiating the comity analysis at step two. A persuasive comity analysis should aim to weave a narrative that takes into account various factors, which can further bolster the case on its merits. For example, in a trade secret misappropriation case, a plaintiff seeking discovery from a Chinese defendant can illustrate how the "bad actor" not only committed the alleged misconduct central to the main dispute (which implicates important US intellectual property interests) but also is using Data Security Laws as an excuse to evade discovery. And any misrepresentation or inconsistent conduct by the defendant can be highlighted as part of this compelling narrative.

For Chinese entities and individuals facing discovery requests, it is crucial to recognize that the Data Security Laws do not serve as an impenetrable shield against discovery obligations in US courts. In particular, the two less stringent compliance measures afforded by the laws—standard contract and personal information protection certification—are unlikely to be considered as a permanent per se bar to discovery. A well-crafted, comprehensive strategy developed early on is the linchpin to a successful defense. In particular, this strategy should address and avoid waiving threshold challenges related to personal jurisdiction and service. A Chinese defendant should also consider utilizing *forum non conveniens* motions, which, if successful, can resolve the case at an early stage. But the mere existence of the Data Security Laws and their potential restrictions or delay on discovery is unlikely to be determinative in the *forum non conveniens* analysis. As the case heads into discovery, a Chinese defendant should be transparent and consider raising the potential data transfer issue and its impact on the case schedule early in the parties' Rule 26(f) conference and case management conference. Early transparency may help prevent estoppel

[53] *Id.*

issues down the road and mitigate the risk of a bad faith finding during the court's comity analysis. And once discovery requests are served, the responding party should promptly seek guidance from the relevant Chinese government authorities, either through the statutorily required procedures or by securing a letter explaining why discovery should not be approved.

Contributors

Kirk K. Nahra
PARTNER

Kirk.Nahra@wilmerhale.com
+1 202 663 6128

Lester Ross
PARTNER

Lester.Ross@wilmerhale.com
+86 10 5901 6363

Allison Bingxue Que
SENIOR ASSOCIATE

Allison.Que@wilmerhale.com
+1 650 858 6007