NOTE

Proportionality and Cross-Border Discovery: A Framework for Reconciling U.S. Discovery Obligations with China's Personal Information Protection Law and Data Security Law

Kent Li†

† New York University, Class of 2022; Cornell Law School, J.D. Candidate, Class of 2027.

Introduction

Cross-border discovery has become one of the most contentious issues in modern transnational litigation. As global business operations generate vast amounts of data stored across multiple jurisdictions, U.S. litigants increasingly seek documents located in countries with restrictive privacy and data-sovereignty regimes.[1] Nowhere is this tension more pronounced than in discovery disputes involving the United States and the People's Republic of China. U.S. courts operate under a historically expansive discovery system that presumes broad access to information and prioritizes the truth-seeking function of litigation.[2] China, by contrast, has constructed a comprehensive regulatory architecture, including the Personal Information Protection Law (PIPL), the Data Security Law (DSL), the Cybersecurity Law, and a series of implementing measures, that strictly regulates data processing and cross-border transfers through purpose limitation, necessity, minimization, and risk-based assessments.[3]

1. Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation* 3 (Jan. 2017), https://www.thesedonaconference.org/sites/default/files/publications/International%2520Litigation%2520Principles_Transitional%2520Ed_Jan%25202017.pdf [https://perma.cc/4PV8-NNE6].

2. Fed. R. Civ. P. 26(b)(1) (pre-2015)(providing that parties may obtain discovery regarding any nonprivileged matter relevant to any party's claim or defense, including the existence, description, nature, custody, condition, and location of documents and other tangible things and the identity and location of persons with knowledge of discoverable matters); Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 351 (1978) ("Relevant" has been broadly construed); *see also* Hickman v. Taylor, 329 U.S. 495, 506-7 (1947)(emphasizing the liberal scope of discovery under the Federal Rules and rejecting attempts to unduly restrict access to relevant information).

3. Personal Information Protection Law of the PRC (2021), arts. 5, 6, 13, 38–43 (establishing core principles for personal information processing, including lawful purpose, necessity, and data minimization, and regulating cross-border transfers of personal information through mechanisms such as security assessments, certification, and standard contractual arrangements)(hereinafter "PIPL").

Data Security Law of the PRC (2021), arts. 3, 21, 25, 31 (Art. 3: defining key terms including "data" and "data processing"; Art. 21: establishing a categorized and graded data protection system; Art. 25: imposing regulatory controls on data processing activities that may affect national security and public interests; Art. 31: requiring risk assessments and regulatory oversight for certain data activities involving national security concerns) (hereinafter "DSL").

Cybersecurity Law of the PRC (2017), arts. 37–40 (localization and security assessments)(hereinafter "Cybersecurity Law").

CAC, Measures for Security Assessment of Cross-Border Data Transfers (2022) (establishing a regulatory framework requiring risk self-assessments and CAC security review for certain outbound transfers of personal information and important data).

These systems are often described as fundamentally incompatible: one rooted in openness and adversarial disclosure, the other grounded in sovereignty, control, and national security.[4]

This Note challenges that conventional narrative. Although the two regimes arise from different legal traditions and reflect distinct policy priorities, both increasingly rely on a common legal principle: proportionality. In the United States, the 2015 amendments to Federal Rule of Civil Procedure 26(b)(1) re-centered proportionality as the core constraint on civil discovery. Courts now evaluate the scope of requests by weighing relevance, burden, cost, access, the importance of the issues at stake, and the value of the information sought, relative to the expense of producing the information.[5] This doctrinal shift has transformed proportionality from a peripheral concept into the dominant analytical framework governing pretrial information exchange.

China's privacy and data-security regime, while grounded in different substantive values, deploys a structurally similar mechanism. The PIPL requires that processing and cross-border transfers be strictly "necessary" for a specified purpose, such as complying with litigation discovery obligations, producing evidence responsive to particular claims or defenses, or supporting expert analysis, and that personal information be limited to the minimum scope required to achieve that purpose.[6] The DSL incorporates similar proportionality-like principles through risk classification, sensitivity-based safeguards, and escalating compliance requirements tied to the volume and importance of the data.[7] Implementing guidelines from the Cyberspace Administration of China further reinforce a balancing inquiry: organizations must justify why the data is needed, assess the risks of transfer, and adopt protective measures calibrated to the nature and sensitivity of the information.[8] Functionally, these requirements mirror the structure of Rule 26(b)(1): both systems demand that the scope of information access be justified by need, and that burdens and risks be weighed against litigants' legitimate objectives.

Understanding this convergence has practical consequences. In most cases, courts either conclude that Chinese privacy and data-security laws do not present a true conflict, or find through comity analysis that U.S. discovery interests outweigh foreign regulatory concerns.[9] This approach often leads

4. Qianwen Zhang, *Conflict Between China's Restrictions on Cross-Border Data Transfer and U.S. Discovery*, 14 Int'l Data Priv. L. 177 (2024); Raymond Yang Gao, *A Battle of the Big Three?—Competing Conceptualizations of Personal Data Shaping Transnational Data Flows*, 22 Chinese J. Int'l L. 707, 712 (2023).

5. Fed. R. Civ. P. 26(b)(1) advisory committee's note to 2015 amendment ("Restores the proportionality factors to their original place. . ."); Oxbow Carbon & Mins. LLC v. Union Pac. R.R., 322 F.R.D. 1, 6–7 (D.D.C. 2017) (applying proportionality factors post-2015).

6. PIPL arts. 5–6, 13 (requiring lawful purpose, necessity, and minimum scope of processing).

7. DSL arts. 21, 24–25, 31 (establishing data classification, graded protection, and sensitivity-based obligations).

8. Outbound Data Transfer Security Assessment Measures (effective Sept. 1, 2022) (Cyberspace Admin. of China); CAC, Guidelines for Security Assessment of Cross-Border Data Transfers (2023) (requiring risk assessments, necessity analysis, and calibrated safeguards).

9. *See* Cadence Design Sys., Inc. v. Syntronic AB, No. 21-CV-03610-SI (JCS), 2022 WL 2290593, at *5 (N.D. Cal. June 24, 2022)(finding no conflict between PIPL and discovery

to full or near-full production of the requested information, but without a consistent framework for reconciling privacy principles across jurisdictions. A proportionality-based analysis provides a more coherent path forward. By incorporating PIPL's necessity and minimization requirements into the existing Rule 26 framework, courts can evaluate cross-border disputes through a shared vocabulary that respects both sovereign interests and adjudicatory needs.[10] Such an approach neither collapses U.S. standards into Chinese law, nor ignores Chinese obligations; instead, it identifies the common structure underlying both systems and unifies the similarities to generate more consistent outcomes.

This Note advances the thesis that U.S. discovery law and China's privacy regime are converging on proportionality as a shared limiting principle, and that this convergence can support a structured judicial rubric for resolving cross-border discovery conflicts. While meaningful differences remain, particularly concerning state secrets, national-security data, and CAC approval requirements, proportionality provides a neutral, trans-systemic lens through which U.S. courts can evaluate requests involving Chinese data, without abandoning the core commitments of either legal system.

I. Evolution of U.S. Discovery Standards

For much of its history, U.S. civil discovery was defined by breadth. Under the pre-2015 version of Rule 26(b)(1), parties could obtain any nonprivileged matter "reasonably calculated to lead to the discovery of admissible evidence."[11] Courts interpreted this language expansively, emphasizing the federal system's commitment to adversarial disclosure and broad access to information. The Supreme Court repeatedly described discovery as "liberal" and "broad," endorsing a presumption of access that favored disclosure over restraint.[12] In practice, once a request satisfied Rule 26's generous relevance threshold, concerns about cost, burden, privacy, and foreign-law conflicts were frequently addressed through objections or protective orders only after production obligations had presumptively attached.[13]

---

obligation because exception applied); Wultz v. Bank of China Ltd., 942 F. Supp. 2d 452, 466–73 (S.D.N.Y. 2013)(finding conflict between PIPL and discovery obligation, but compelling production after comity analysis favored U.S. discovery interests).

10. *See* Ingrid Brunk, *Applying Foreign Data Protection Laws: Greater Impact on U.S. Discovery Than Foreign Blocking Statutes*, Transnat'l Litig. Blog (Oct. 25, 2022), https://tlblog.org/foreign-data-protection-laws-greater-impact-on-u-s-discovery-than-foreign-blocking-statutes [https://perma.cc/ZQ6K-73W5].

11. Fed. R. Civ. P. 26(b)(1) (pre-2015)

12. Oppenheimer Fund, Inc., 437 U.S. at 351; Seattle Times Co. v. Rhinehart, 467 U.S. 20, 34 (1984).

13. Fed. R. Civ. P. 26(b)(1) advisory committee's note to 2015 amendment (discussing the 2000 addition of the sentence in Rule 26(b)(1) providing that "[a]ll discovery is subject to the limitations imposed by Rule 26(b)(2)(C)," and explaining that this "otherwise redundant cross-reference" was added to encourage "active judicial use" of proportionality limits); Robert D. Keeling & Ray Mangum, *The Burden of Privacy in Discovery*, 105 Judicature 66, 67 (2021), https://judicature.duke.edu/articles/the-burden-of-privacy-in-discovery [https://perma.cc/Q8VZ-6PA7]; Matthew T. Ciulla, *A Disproportionate Response? The 2015*

Over time, however, the broad-access model generated substantial practical and normative concerns.[14] Judges and litigants increasingly described discovery as one of the most expensive and contentious components of federal litigation, particularly in cases involving electronically stored information ("ESI").[15] The rise of multinational corporations and cloud-based storage amplified these burdens: parties were now required to collect, review, and produce data distributed across multiple jurisdictions, sometimes in countries with blocking statutes or data-sovereignty laws. The Advisory Committee on Civil Rules observed that the "reasonably calculated" formulation had been misused to justify disproportionate discovery and had contributed to escalating costs that bore little relationship to the needs of the case.[16] These dynamics set the stage for a doctrinal shift.

The 2015 amendments to Rule 26(b)(1) (hereinafter the "Current Rule 26(b)(1)") represent the most significant recalibration of federal discovery in decades. The amendments deleted the "reasonably calculated" language, representing a deliberate repudiation of the phrase, and placed proportionality at the core of the discovery standard.[17] Under the Current Rule 26(b)(1), parties may obtain only information that is both relevant and "proportional to the needs of the case," evaluated through six factors: (1) "the importance of the issues at stake", (2) "the amount in controversy", (3) "the parties' relative access to information", (4) "the parties' resources", (5) "the importance of the discovery in resolving the issues", and (6) "whether the burden or expense outweighs the likely benefit."[18] Proportionality is no longer an affirmative defense; it is an integral component of the requesting party's burden.

Post-amendment case law reflects this shift. Courts repeatedly stress that proportionality demands a holistic, commonsense assessment of the Current Rule 26(b)(1) factors, not a mechanical cost-benefit calculation. In *Oxbow Carbon & Minerals LLC v. Union Pacific Railroad*, the court granted a motion to compel after weighing each proportionality factor and rejecting the argument that expense alone rendered otherwise relevant discovery disproportionate.[19] Similarly, in *In re Bard IVC Filters Products Liability Litigation*, the court

---

Proportionality Amendments to Federal Rule of Civil Procedure 26(b), 92 Notre Dame L. Rev. 1395, 1411-13 (2017).

14. Memorandum from Judge David G. Campbell, Chair, Advisory Comm. on Fed. Rules of Civil Procedure, to Judge Jeffrey Sutton, Chair, Standing Comm. on Rules of Practice and Procedure 6–7 (June 14, 2014), http://www.uscourts.gov/file/18218/ [https://perma.cc/WAN6-B3TW](reporting Federal Judicial Center survey results indicating that 58.2% of defense-side lawyers believed litigation costs, including discovery, had caused at least one client to settle a case that otherwise would not have settled, and that a quarter of attorneys viewed discovery costs as too high relative to the stakes of the case).

15. *See* Thomas E. Willgin & Emery G. Lee III, *In Their Words: Attorney Views About Costs and Procedures in Federal Civil Litigation*, Fed. Judicial Center 14-16 (Mar. 2010), https://www.uscourts.gov/file/3283/download [https://perma.cc/CR5E-HDKP]; Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 318–20 (S.D.N.Y. 2003) (describing costs associated with ESI).

16. Fed. R. Civ. P. 26(b)(1) advisory committee's note to 2015 amendment.

17. *Id.* ("The 'reasonably calculated' phrase has continued to create problems. . .")

18. Fed. R. Civ. P. 26(b)(1).

19. Oxbow Carbon & Minerals LLC v. Union Pacific Railroad, 322 F.R.D. 1, 6, 11 (D.D.C. 2017).

explained that proportionality under amended Rule 26(b)(1) is not a requirement imposed only in resolving disputes, but one for which "[t]he parties and the court have a collective responsibility to consider . . . all discovery" and to apply in making "a case-specific determination of the appropriate scope of discovery."[20] Courts have also incorporated foreign-law complications into proportionality analysis, treating privacy and data-sovereignty restrictions as part of the burden and risk side of the balance.[21]

Taken together, the doctrinal evolution of Rule 26 demonstrates a clear movement away from expansive, relevance-driven discovery and toward a structured, burden-sensitive approach.[22] Proportionality now functions as the central organizing principle of federal discovery, one that mediates between litigants' need for information and competing interests such as cost, efficiency, privacy, and compliance with foreign law.[23] This shift provides the analytical foundation for harmonizing U.S. discovery with restrictive international data-protection regimes, and sets the stage for comparing the Current Rule 26(b)(1) with China's necessity and minimization-based privacy framework.

II. Overview of China's PIPL and DSL

Before the enactment of the Personal Information Protection Law (PIPL) and the Data Security Law (DSL), China's approach to personal information and data security was fragmented and largely indirect.[24] Privacy protections were dispersed across sectoral regulations, general civil-law principles, national standards, and the 2017 Cybersecurity Law, rather than consolidated in a single, comprehensive statute.[25] As a result, restrictions on data handling and cross-border transfers were often articulated through sovereignty-based controls such as state secrecy laws, banking confidentiality obligations, and limits on providing evidence to foreign courts, rather than through an explicit, system-wide framework of necessity and minimization.[26] In cross-border

20. In re Bard IVC Filters Prods. Liab. Litig., 317 F.R.D. 562, 564-65 (D. Ariz. 2016) (citing Rule 26, Advis. Comm. Notes for 2015 Amends.)

21. *See, e.g.,* Wultz v. Bank of China Ltd., 942 F. Supp. 2d at 467–68 (evaluating the burden imposed by Chinese secrecy laws and nonetheless ordering production of documents located in China after finding the requested discovery crucial to determining whether the bank had notice that the accounts were funding terrorism and that no alternative sources existed for the evidence).

22. Ciulla, *supra* note 13, at 1400-05.

23. *Id.* at 1410.

24. Graham Greenleaf, *China's Completed Personal Information Protection Law: Rights Plus Cyber-Security*, 172 Privacy Laws & Bus. Int'l Rep. 20, 20–23 (2021) (describing PIPL as "the culmination of a decade of incremental reform" and explaining that the final framework makes China's personal data rules less ambiguous); *see also* Rogier Creemers, *China's Emerging Data Protection Framework,* 8 J. Cybersecurity 3 (2022).

25. *See* Cybersecurity Law, *supra* note 3; Ministry of Industry & Information Technology, Telecommunications and Internet Personal User Data Protection Regulations (Order No. 24) (promulgated July 16, 2013, effective Sept. 1, 2013) (PRC) (reflecting pre-PIPL sectoral regulation).

26. *See* Civil Procedure Law of the People's Republic of China, art. 277 (restricting foreign entities from collecting evidence within China "without permission from the competent authorities").

litigation, this landscape produced a binary dynamic between two competing legal logics: U.S. discovery demands grounded in broad relevance standards confronted Chinese objections framed primarily in terms of secrecy and territorial control, with courts resolving disputes through ad hoc comity analysis rather than through parallel limitation principles such as necessity, proportionality, and data minimization that systematically constrain data access in both legal regimes.[27] The enactment of the PIPL and DSL marks a decisive shift away from this patchwork toward a unified, statutory regime that expressly structures data access around necessity, risk, and proportionality.[28] Just as the 2015 amendments to Rule 26(b)(1) transformed U.S. discovery by recentering proportionality as an organizing principle, China's post-2021 data laws formalize a comparable movement toward structured limitation in data governance, setting the stage for meaningful comparison between the two systems.[29]

PIPL begins with a foundational principle that personal information processing must be lawful, justified, and limited in scope. Article 5 requires that processing be conducted in a manner that is "lawful, justified, necessary, and with good faith," and that it be "limited to the minimum scope necessary to achieve the purpose of processing."[30] Article 6 reinforces this by mandating that processing be directly related to a specified and reasonable purpose, and that it have "the smallest impact on individuals' rights and interests."[31] These provisions embed a form of necessity and minimization akin to proportionality: organizations must both articulate why data is needed and ensure that the volume and intrusiveness of processing are no greater than required.

PIPL's legal bases for processing, set out in Article 13, further operationalize necessity. Processing is permitted only under enumerated grounds, such as consent, performance of a contract, fulfillment of statutory duties, or responses to public health or emergency events, and even then must be "within a reasonable scope" necessary to achieve the stated purpose.[32] Sensitive personal information, defined in Article 28 to include data such as biometric identifiers, medical information, and location tracking, triggers heightened obligations, including a "specific purpose and sufficient necessity" standard and stricter protective measures.[33] These graduated requirements reflect a risk-based proportionality structure: the more sensitive the data, the stronger the justification and safeguards required.

The DSL extends this logic beyond personal information to encompass data generally. It introduces a national data-classification and grading system that distinguishes among ordinary data, "important data," and "national core data" based on their potential impact on national security, the public interest,

27. *See* Société Nationale Industrielle Aérospatiale for Southern Dist. of Iowa, 482 U.S. 522 (1987) (comity balancing framework); Wultz v. Bank of China Ltd., 910 F. Supp. 2d at 459, 466 (applying comity factors to Chinese secrecy/bank-law objections).

28. *See generally* PIPL; DSL.

29. Fed. R. Civ. P. 26(b)(1) advisory committee's note to 2015 amendment (re-centering proportionality); *see also* PIPLarts. 5–6 (necessity/minimization principles) (supporting the comparison that both regimes formalize structured limitation).

30. PIPL art. 5.

31. *Id.* art. 6.

32. *Id.* art. 13.

33. *Id.* arts. 28–29.

and economic development.[34] Article 21 requires that data processing be conducted in accordance with a data-security management system, with organizations conducting risk assessments and adopting appropriate technical and organizational measures.[35] Article 31 requires risk assessments and reporting obligations when data processing activities may affect national security.[36] These provisions do not use the term "proportionality," but effectively require decision-makers to calibrate safeguards and controls to the sensitivity and potential harm associated with the data.

Cross-border data transfers are subject to additional, explicitly risk-based mechanisms that further illustrate the proportionality structure. Under PIPL Articles 38–43, personal information may be transferred overseas only if at least one of several conditions is met: passing a CAC-organized security assessment, concluding a standard contract in the form issued by CAC, obtaining certification from a recognized body, or satisfying other conditions prescribed by law.[37] Large-scale transfers or transfers involving critical information infrastructure operators generally must undergo CAC security assessments, which require organizations to analyze the necessity of the transfer, the volume and sensitivity of the data, the risks of leakage or misuse, and the adequacy of contractual and technical safeguards.[38] The CAC Measures for Security Assessment of Cross-Border Data Transfers and associated guidelines specify that assessments must consider factors such as the purpose of transfer, the type and scale of data, the risks posed by the recipient's jurisdiction, and the impact on national security and public interests.[39]

These mechanisms operate as proportionality filters. Before data may leave China, organizations must demonstrate that the transfer is necessary for a defined purpose, that the scope of data is limited to what is required, and that the risks are mitigated through appropriate safeguards. The more sensitive or voluminous the data, the more stringent the procedural steps and protective measures become. Scholars and practitioners have accordingly described China's regime as embedding a "necessity and minimization" model that balances data flows against privacy and security concerns, even while emphasizing sovereignty and control.[40]

For purposes of cross-border discovery, these statutory requirements function much like proportionality constraints in litigation. They do not categorically bar the export of information, but require a granular assessment of why particular data must be transferred, whether the same objectives can be achieved through less intrusive means (such as redaction or in-country

34. DSL arts. 2, 21, 24, 25, 31.
35. *Id.* art. 21.
36. *Id.* art. 31.
37. PIPL arts. 38–40.
38. *Id.* art. 40; *see also* DSL art. 31.
39. Outbound Data Transfer Security Assessment Measures (effective Sept. 1, 2022) (Cyberspace Admin. of China), art. 5(1); CAC, Guidelines for Security Assessment of Cross-Border Data Transfers (2023).
40. *See, e.g.,* Jamie P. Horsley, *China's Data Dilemma: Maximizing Data Utilization While Ensuring Data Security*, Yale L. Sch. Paul Tsai China Ctr. 11 (Oct. 25, 2025), https://law.yale.edu/sites/default/files/area/center/china/document/horsley-chinas-data-dilemma-ssrn-5674524.pdf [https://perma.cc/R69N-8DAJ].

review), and what safeguards are needed to reduce the risk of harm.[41] When U.S. courts encounter PIPL- or DSL-based objections, they are thus interfacing with a legal regime that already incorporates structured necessity and risk-balancing as gatekeeping principles. This functional structure provides a natural point of comparison with Current Rule 26(b)(1)'s proportionality analysis and suggests that, despite differences in terminology and underlying values, both systems rely on similar logic to limit overbroad access to information.

III. U.S. Courts and Corporate Practice in Applying Proportionality to Chinese Data Laws

A. U.S. Courts Confront Chinese Privacy and Data-Security Laws

U.S. courts evaluate objections grounded in Chinese privacy and data-security laws within the general framework governing transnational discovery. In *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*, the Supreme Court rejected categorical rules that would either require resort to the Hague Evidence Convention or treat foreign law as a dispositive bar to discovery.[42] Instead, the Court held that disputes implicating foreign sovereign interests call for a fact-specific comity analysis that accommodates those interests, without displacing the Federal Rules.[43] *Aérospatiale* thus established the basic framework that continues to govern how U.S. courts evaluate transnational discovery requests and objections grounded in foreign law.

In *Aérospatiale*, the Court explained that the Hague Evidence Convention provides optional, rather than exclusive, procedures for obtaining evidence abroad and that district courts retain authority to order parties within their jurisdiction to produce foreign-located evidence.[44] The Court declined to adopt a blanket "Hague-first" rule, emphasizing that comity does not require courts to adhere to Convention procedures in every case, particularly where those mechanisms may be slower, more costly, or less effective than discovery under the Federal Rules.[45] At the same time, *Aérospatiale* made clear that foreign law remains a relevant consideration. Courts must conduct a "particularized analysis" of the circumstances, weighing factors such as the importance and specificity of the requested information, the availability of alternative means of obtaining it, and the relative strength of U.S. and foreign sovereign interests. Trial courts are further instructed to exercise "special vigilance" in supervising

41. *See* PIPL arts. 38–40 (requiring security assessments and appropriate safeguards before personal information may be transferred abroad); DSL art. 31 (requiring risk assessments and security management measures for certain data processing activities); CAC, *Measures for Security Assessment of Cross-Border Data Transfers* art. 5 (requiring data handlers to conduct risk self-assessments evaluating the legality, necessity, and potential risks of outbound data transfers).

42. Société Nationale Industrielle Aérospatiale, 482 U.S. at 522.

43. *Id.* at 544-46.

44. *Id.* at 532-40.

45. *Id.* at 542-43.

cross-border discovery, both to prevent abusive practices and to avoid imposing unnecessary or disproportionate burdens on foreign litigants.[46]

Pre-PIPL decisions involving Chinese bank-secrecy and state-secrets rules illustrate how courts have operationalized this approach. In *Wultz v. Bank of China Ltd.*, plaintiffs sought bank records to support terrorism-financing claims. Bank of China argued that production would violate Chinese bank-secrecy law and expose it to sanctions. Judge Scheindlin applied an expanded *Aérospatiale* comity analysis and concluded that the United States' interest in enforcing its anti-terrorism laws, the centrality of the requested evidence, and the absence of effective alternatives outweighed the speculative risk of Chinese enforcement, ultimately compelling substantial production.[47] At the same time, the court approved targeted redactions and protective measures for certain investigative materials, showing that comity could be expressed through narrowing the scope of productions and imposing safeguards, rather than outright denial of discovery.[48]

The enactment of the PIPL and DSL has not fundamentally altered this trajectory. In *Cadence Design Systems, Inc. v. Syntronic AB*, a Northern District of California case, the defendant argued that PIPL Article 39 required employee consent before complying with the discovery request to ship computers located in China to the United States for forensic inspection. Magistrate Judge Spero held that PIPL did not bar compliance with the court's prior discovery order, relying on Article 13's exception for processing "necessary to fulfill statutory duties and responsibilities or statutory obligations."[49] The court interpreted "statutory obligations" to include foreign legal obligation (encompassing compliance with U.S. discovery orders), and noted the lack of any authority showing that China had imposed sanctions on parties for following foreign court orders.[50]

A year later, in *Owen v. Elastos Foundation*, Magistrate Judge Moses in the Southern District of New York reached a similar conclusion. The defendants invoked PIPL to justify withholding communications stored on devices in China. The court first held that PIPL did not apply to certain data stored outside China because the processing was not directed at individuals in China. For information inside China, the court again relied on Article 13(3)'s exception for statutory obligations to conclude that complying with U.S. discovery did not violate PIPL.[51] In the alternative, Judge Moses conducted a full Aérospatiale/Wultz comity analysis and ordered production even assuming a conflict, emphasizing the importance of the information to securities-fraud claims, the lack of effective alternative means, and the absence of evidence that PIPL had been enforced against parties for obeying U.S. discovery orders.[52]

Commentators have observed that courts often treat PIPL and DSL much like earlier "blocking statutes," a category of foreign laws that restrict

46. *Id.* at 546.
47. Wultz v. Bank of China Ltd., 942 F. Supp. 2d at 454.
48. *Id.* at 473.
49. Cadence Design Sys. Inc., 2022 WL 2290593, at *5.
50. *Id.* at *5-6.
51. Owen v. Elastos Found., 343 F.R.D. 268, 285-86 (S.D.N.Y. 2023).
52. *Id.* at 286-89.

the disclosure of information to foreign courts, such as state-secrecy laws, bank-confidentiality rules, or statutes limiting the transfer of evidence abroad. As with those statutes, the laws are typically treated as relevant to comity analysis but rarely outcome-determinative.[53] In addition, practitioner commentary notes that efforts to invoke DSL Article 36 and PIPL Article 41 as categorical bars have mostly failed, with courts declining to recognize an "automatic shield" against U.S. discovery and instead folding Chinese laws into proportionality and comity analysis.[54] So far, the available case law suggests that U.S. courts will continue to order production where the information is important, alternatives are limited, and the risk of actual Chinese enforcement is uncertain or speculative.

B. Corporate Practice: Operationalizing Proportionality Through Redaction, In-Country Review, and Data Minimization

Faced with these judicial trends and the real possibility of conflicting legal obligations, corporate actors have developed practices that operationalize proportionality on the ground.[55] These techniques, including redaction, in-country review, and data minimization, aim to satisfy U.S. discovery obligations while reducing the volume and sensitivity of data that must cross borders.

First, in-country collection and review have become a common tool in cross-border discovery involving China. The Sedona Conference, a nonprofit research institute whose working groups produce widely cited best-practice guidance on e-discovery and cross-border data issues, in its *Practical In-House Approaches for Cross-Border Discovery & Data Protection* (hereinafter "The Sedona Practical Approaches Document") urges companies to plan "successful in-country collection" by mapping local systems, coordinating with local business units, and conducting review within the originating jurisdiction before any transfer occurs.[56] In practice, multinational corporations frequently host review platforms in China or engage local e-discovery vendors so that initial culling, keyword filtering, and responsiveness review are performed locally.[57] Only a subset of documents deemed responsive and necessary for the litigation are exported, often after additional filtering or anonymization.[58] This structure aligns with PIPL's emphasis on necessity and minimization while allowing parties to meet U.S. production deadlines.

Second, redaction and anonymization serve as key proportionality tools. Both Chinese regulators and international best-practice guidance recognize

53. William S. Dodge, *Another Court Rejects Chinese Data Privacy Law as a Bar to U.S. Discovery*, Transnat'l Litig. Blog (Mar. 1, 2023), https://tlblog.org/another-court-rejects-chinese-data-privacy-law-as-a-bar-to-u-s-discovery [https://perma.cc/HM9H-U9HT].

54. Davis & Gao, *Conducting Investigations and Discovery in China: What Companies Need to Consider in Preparing for New Policies*, Alm Law.Com (Mar. 26, 2025), https://www.crowell.com/a/web/3PNVHe4SmgFaXnoQKFd8c9/cc328202562977crowell.pdf [https://perma.cc/B86J-ER2F].

55. Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, 17 Sedona Conf. J. 397, 403 (2016).

56. *Id.* at 419–25.

57. *Id.* at 422-24.

58. *Id.* at 424-25.

that removing direct identifiers or masking sensitive fields can mitigate privacy risks, while preserving evidentiary value.[59] The Sedona Practical Approaches Document recommends using the processing and review stages to limit the production of protected data, and to implement safeguards for any protected information that must be disclosed.[60] In China-related matters, this often means redacting national ID numbers, home addresses, and nonessential employee data, or substituting unique identifiers in place of names. Courts have accepted such approaches in other cross-border cases, and have used protective orders to reinforce confidentiality. These decisions signal that narrowed, redacted productions are consistent with both proportionality and comity.[61]

Third, data minimization and phased production implement proportionality in a more structural way. Rather than exporting entire mailboxes or file shares, companies design collection protocols that target custodians and time periods most likely to yield relevant evidence. Sedona's international guidance encourages parties to "stage" discovery. This means first producing less sensitive and more clearly relevant categories, and expanding only if necessary.[62] In cases involving Chinese data, phased production may begin with providing information from U.S.-based custodians and nonpersonal business records, followed by narrower requests for Chinese custodians' documents, and only as a last resort, highly sensitive or regulated categories. This sequencing reduces the volume of data subject to PIPL/DSL, and provides a factual record to show courts that parties have attempted less intrusive means before seeking broader transfers.

These corporate practices both respond to and shape judicial expectations. When courts apply comity factors and consider Chinese law within that framework, they often look to whether parties have tried reasonable mitigation measures in good faith, before asserting that foreign law makes production impossible.[63] Companies that can demonstrate thoughtful, risk-based processes grounded in recognized frameworks like The Sedona Conference's International Principles and The Sedona Practical Approaches Document are better positioned to argue that any remaining conflict is genuine and that

59. *Id.* at 424–25; *see also* Sedona Conference International Principles, *supra* note 1, at 18.

60. Sedona Conference, *supra* note 55, at 423-25.

61. *See* In re DiDi Glob. Inc. Sec. Litig., No. 21-CV-5807 (LAK), 2025 WL 743964, at * 3 (S.D.N.Y. Mar. 7, 2025)(denying a request to compel broad production of redacted and withheld documents, requiring a revised withhold log, and directing plaintiffs to identify specific documents and demonstrate their importance and the absence of alternative sources before further production would be ordered); Wultz v. Bank of China Ltd., 942 F. Supp. 2d at 473 (compelling production, but permitting targeted redactions and requiring in camera review/production under seal for sensitive materials).

62. The Sedona Conference, *supra* note 55, at 438-39, 446-47; The Sedona Conference International Principles, *supra* note 1, at 17-8.

63. *See* In re Valsartan, Losartan, & Irbesartan Prods. Liab. Litig., No. MDL 2875 (RBK), 2021 WL 6010575, at *17 (D.N.J. Dec. 20, 2021)(considering whether the resisting party had acted in good faith by consulting Chinese counsel and seeking guidance from Chinese authorities before invoking state-secrets law as a basis for withholding discovery); Owen v. Elastos Found., 343 F.R.D. at 285((noting that defendants had attempted to comply with both U.S. discovery obligations and Chinese law, including efforts to obtain custodian consent and consult Chinese legal experts).

further accommodations are warranted. Conversely, courts have been less receptive when parties invoke foreign law as a bare slogan without offering concrete, proportionate alternatives, or a cognizable threat that complying with U.S. discovery will result in domestic penalties.[64]

In short, U.S. case law and corporate practice are converging on a similar operational logic: conflicts with Chinese privacy and data-security laws are to be managed, as far as possible, through proportional narrowing and technical safeguards rather than by halting discovery altogether. This convergence provides the practical foundation for the proportionality-based rubric proposed in Part IV.

IV. Proportionality as a Bridging Framework: A Model Rubric for U.S.–China Discovery

A. From Conflict to Convergence: Reframing the Analytical Lens

Cross-border discovery disputes involving China are often presented as a direct collision between two systems: broad U.S. disclosure obligations on one side and restrictive Chinese privacy and data-security rules on the other.[65] But as Parts II and III show, this conflict framing can obscure what is most legally useful for courts: both Current Rule 26(b)(1) and the PIPL rely on limitation principles that require justification, narrowing, and risk-sensitive calibration. As the case law illustrates, Chinese privacy and data-security laws rarely operate as dispositive constraints on discovery. Courts most often resolve disputes either by finding no true conflict, or by concluding that comity considerations favor U.S. disclosure obligations.[66] The result is that production typically proceeds,but without a consistent framework explaining how foreign-law limitations should shape discovery scope, sequencing, or protective safeguards.

A more predictable approach begins by treating Chinese privacy law as analytically compatible with the U.S. discovery framework. This does not mean importing Chinese law wholesale into federal procedure, nor does it require courts to abandon *Aérospatiale*'s comity inquiry. Instead, it means recognizing that proportionality is already the central organizing principle of U.S. discovery and that PIPL objections frequently supply information that is directly relevant to proportionality: the sensitivity of the data, the scale of the transfer, the

64. Nidec Motor Corp. v. Broad Ocean Motor, LLC, No. 4:13-CV-01895-SEP, 2023 WL 346027, at *3 (E.D. Mo. Jan. 20, 2023)(rejecting reliance on Chinese law where defendants offered only speculative claims of potential penalties and failed to identify any concrete instance in which a party had been sanctioned for complying with U.S. discovery); Christopher Boehning & Daniel J. Toal, *Absent Document Requests, Court Rejects Hypothetical Challenges in GDPR Dispute*, N.Y. L.J. (Dec. 1, 2025), https://www.paulweiss.com/media/srabrmb0/nylj_boehning_toal_absent_document_requests_court_rejects_hypotherical_challenges_in_gdpr_dispute.pdf#:~:text=in%C2%A0%20Sowa%20v.%20Mercedes,Courts%20are%20reluctant [https://perma.cc/R4KW-WDDQ].

65. Zhang, *supra* note 4, at 181-82; Gao, *supra* note 4.

66. *See* Cadence Design Sys., Inc., 2022 WL 2290593, at *5 (finding no conflict between PIPL and discovery obligation because exception applied); Wultz v. Bank of China Ltd., 942 F. Supp. 2d at 466–73 (finding conflict between PIPL and discovery obligation, but compelling production after comity analysis favored U.S. discovery interests).

compliance burden, and the availability of less intrusive alternatives. In short, courts can reduce uncertainty by treating PIPL not as an external veto,[67] but as a structured set of constraints that can be operationalized through familiar Rule 26 tools.

B. Mapping Current Rule 26(b)(1) to PIPL's Necessity and Minimization Framework

Current Rule 26(b)(1) authorizes discovery only if it is both relevant and "proportional to the needs of the case," considering (among other factors) the importance of the issues, the parties' relative access to the information, the importance of the discovery in resolving the issues, and whether the burden or expense outweighs the likely benefit.[68] PIPL, meanwhile, requires that personal information processing be lawful and "necessary" and that it be limited to the "minimum scope necessary" to achieve the stated purpose.[69] Even though these regimes emerged from distinct legal traditions[70], their functional logic aligns in ways that are especially salient to cross-border discovery.

First, PIPL's necessity requirement parallels Current Rule 26(b)(1)'s emphasis on the *importance* of the discovery to resolving the dispute. If a category of personal information is marginally relevant or duplicative, proportionality analysis already empowers courts to deny it as unnecessary or to require a narrower alternative; PIPL's necessity framing simply reinforces that the requesting party should be able to explain why the requested categories are truly needed.[71]

Second, PIPL's minimization principles track Rule 26's "burden versus benefit" factor. Where a request sweeps in large volumes of personal information, minimization pushes toward narrowing the scope of production by custodian, time period, data field, and sensitivity. Those same narrowing moves are the standard mechanisms by which federal judges enforce proportionality in domestic ESI disputes.[72]

---

67. Dodge, *supra* note 53 (Treating PIPL as an external veto as an external veto would be similar to treating PIPL as a blocking statute, which courts routinely decline to treat as a meaningful obstacle to compelled production.)

68. Fed. R. Civ. P. 26(b)(1).

69. PIPL arts. 5–6.

70. The U.S. discovery system is rooted in the common-law adversarial tradition, under which broad pre-trial disclosure serves the litigation system's truth-seeking function. *See* Hickman v. Taylor, 329 U.S. 495, 507 (1947); China's data governance framework, by contrast, operates in what Creemers describes as a "teleological, instrumental legal environment" in which "the very notion of a fundamental right is absent," and in which data regulation is oriented toward state security and national development rather than individual rights. Creemers, *supra* note 24, at 2; *see also* Gao, *supra* note 4, at 711, 722 (describing China's primary conceptualization of personal data as "an element of national security" supporting a "security-oriented" regulatory regime); DSL art. 1 (stating that the law is enacted to "safeguard the sovereignty, security, and development interests of the state").

71. Fed. R. Civ. P. 26(b)(2)(C)(i) (requiring courts to limit discovery that is "unreasonably cumulative or duplicative"); PIPL art. 6 (requiring that processing be "directly related to" its stated purpose and "limited to the minimum scope required").

72. *See* Muslims on Long Island, Inc. v. Town of Oyster Bay, No. 25-CV-00428 (SJB) (JMW), 2025 WL 1582250, at *5 (E.D.N.Y. June 4, 2025)(limiting discovery of personal devices absent specific evidence of relevant communications); Winfield v. City of

Third, PIPL's and China's implementing rules introduce a risk-calibrated compliance architecture for cross-border transfers (e.g., heightened safeguards for sensitive personal information and security assessment mechanisms for certain outbound transfers).[73] In Rule 26 terms, those risk- and compliance-based obligations belong on the "burden/expense" side of the proportionality balance, alongside the familiar costs of preservation, review, and production. Treating PIPL compliance burdens as part of proportionality does not privilege foreign law over U.S. discovery; it simply treats regulatory risk and compliance burdens as a real-world cost of production that Rule 26 already instructs courts to weigh.[74] Finally, both systems implicitly encourage courts and parties to consider less intrusive alternatives before ordering maximal disclosure. PIPL's minimization and sensitivity structure invites alternatives like redaction, pseudonymization(replacing identifying information with pseudonyms while preserving usability of the data), and in-country review; Rule 26's proportionality framework and protective-order authority provide the doctrinal tools to implement those alternatives in litigation.[75]

C. A Single Integrated Rubric: Necessity Showings + Phased Production + Calibrated Safeguards

Recognizing this functional overlap is useful only if it produces an administrable method that courts can apply consistently. Building on existing Rule 26 doctrine and the recurring patterns in China-related disputes, courts should adopt a single integrated rubric that combines several familiar discovery tools with three linked components: (1) structured necessity showings, (2) phased and scoped production, and (3) calibrated protective measures. Each component is familiar in U.S. discovery practice;[76] the rubric simply standardizes how they are deployed when PIPL/DSL issues are raised.

1. Structured Necessity Showings (Creating a Reliable Record)

When Chinese privacy or data-security objections are asserted, courts should require structured necessity showings from both sides before determining discovery scope. On the requesting side, this requires identifying the categories of information sought, by custodian, timeframe, and data type, and explaining why narrower sources are inadequate to prove or defend concrete claims or defenses, consistent with Current Rule 26(b)(1) and

New York, No. 15-CV-05236(LTS)(KHP), 2018 WL 840085, at *8 (S.D.N.Y. Feb. 12, 2018) (limiting discovery to a limited time period to ensure proportionality and avoid ongoing data updates).

73. PIPL arts. 28–29 (sensitive personal information), 38–43 (cross-border transfers); Outbound Data Transfer Security Assessment Measures (effective Sept. 1, 2022) (Cyberspace Admin. of China).

74. *See* Fed. R. Civ. P. 26(b)(1) (burden/expense vs. likely benefit).

75. Fed. R. Civ. P. 26(c); PIPL arts. 5–6, 28–29.

76. *See, e.g.,* Fed. R. Civ. P. 26(b)(1) (proportionality and relevance); Fed. R. Civ. P. 26(c) (protective orders); Fed. R. Civ. P. 26(f) (requiring parties to develop a discovery plan addressing the scope and sequencing of discovery)

Rule 26(g)'s certification duties.[77] On the responding side, it requires more than citing "PIPL" in the abstract. The responding party should identify the specific PIPL or DSL provisions implicated, the sensitivity and volume of the data at issue, and the compliance steps it proposes as less intrusive alternatives, such as redaction, anonymization, in-country review, or staged production.[78]

In practice, these obligations can be implemented through a focused, evidence-based record. Courts can require the requesting party to submit a data map linking each category of requested information to a specific claim or defense and identifying the least intrusive means of obtaining it. The responding party would then provide a parallel burden-and-risk showing identifying where the data is stored, estimating the volume implicated, and explaining why particular PIPL or DSL provisions are triggered. Courts have repeatedly emphasized that proportionality is not satisfied by abstract invocations of burden or foreign law.[79] Rather, the party asserting a legal conflict must provide concrete information, while the requesting party must explain why the discovery is important to resolving the dispute.[80] This record-building approach operationalizes PIPL's necessity and minimization principles, while remaining fully consistent with Current Rule 26(b)(1)'s allocation of responsibility and Rule 26(g)'s certification obligations.[81]

2. *Phased and Scoped Production (Testing Necessity Before Expanding Exposure)*

Courts should default to sequenced discovery plans that (a) prioritize U.S.-based or low-risk sources first, (b) then move to more targeted categories of China-stored data, and (c) reach sensitive/high-risk categories only if earlier phases demonstrate that they are truly necessary. Rule 26 expressly contemplates judicial control over the sequence and timing of discovery, and phased discovery is a standard proportionality tool in ESI-heavy cases.[82] Phasing serves several functions in the China context. It reduces unnecessary cross-border transfer; it creates a factual record showing what information is actually needed; and it buys time for parties to complete compliance-oriented

77. Fed. R. Civ. P. 26(g)(1)(B) (certification that discovery requests and responses are consistent with the rules, and not unreasonable or unduly burdensome).

78. See PIPL arts. 5–6 (requiring a lawful purpose, necessity, and data minimization in personal information processing); art. 13 (providing the legal bases for processing personal information); arts. 38–40 (imposing conditions and safeguards for cross-border transfers of personal information).

79. In re Grand Jury Proc., 873 F.2d 238, 239–40 (9th Cir. 1989) (burden on party relying on foreign law to show that the law "bars compliance with a court order").

80. Société Nationale Industrielle Aérospatiale, 482 U.S. at 544 (citing Restatement (Third) of Foreign Relations Law of the United States § 437(1)(c) as identifying factors relevant to comity analysis, including the importance of the documents to the litigation).

81. Fed. R. Civ. P. 26(g)(1)(B).

82. Fed. R. Civ. P. 26(d) (timing and sequence of discovery); Fed. R. Civ. P. 26(f) (discovery plan); *see also* Coventry Cap. U.S. LLC v. EEA Life Settlements Inc., No. 17 Civ. 7417 (VM) (SLC), 2020 WL 7383940, at *10 (S.D.N.Y. Dec. 16, 2020) (ordering phased ESI discovery, including initial targeted custodians and search-term testing before determining whether broader production was warranted).

steps (such as in-country review or internal risk assessments) without halting the litigation. International best-practice guidance likewise emphasizes in-country collection, disciplined processing, and limiting production of protected data when feasible. These are measures that become more effective when courts structure discovery in phases, rather than ordering immediate, maximal production.[83]

Functionally, this approach translates into discovery orders that define both scope and checkpoints ex ante.[84] A court might order an initial phase limited to a small number of high-yield custodians, a narrow time period, and non-sensitive business records, with production confined to specified repositories or data fields. The order can then require the parties to meet and confer after that phase to assess what the production yielded; for example, whether key documents were identified, whether gaps remain, and whether narrower alternatives have been exhausted, before permitting any expansion. If additional discovery is warranted, the court can incrementally add custodians, extend date ranges, or authorize production of more sensitive categories, often subject to heightened safeguards.[85] By tying each expansion to demonstrated need, courts ensure that broader cross-border transfers occur only after less intrusive means have been tested and found inadequate.

3. *Calibrated Protective Orders and Technical Safeguards (Reducing Risk While Enabling Production)*

Finally, courts should treat protective measures as variables that can shift the proportionality balance. Rule 26(c) authorizes protective orders to shield parties from undue burden and to protect confidential or sensitive information.[86] The U.S. Supreme Court has recognized that such orders are often necessary to manage the risks inherent in broad discovery.[87] In cross-border discovery dispute involving China, calibrated measures may include: attorneys'-eyes-only restrictions; secure review platforms; limits on

83. Sedona Conference, *supra* note 55, at 423-24 (June 2016) (recommending in-country collection planning and limiting production of protected data where possible).

84. *See* Fed. R. Civ. P. 26(b)(1), (d); Fed. R. Civ. P. 26 advisory committee's note to 2015 amendment (integrating proportionality into the definition of discovery scope and emphasizing judicial management); *Id.*(advisory committee's note to 1970 amendment (confirming the court's authority to structure the sequence and timing of discovery).

85. *See* Sedona Conference, *supra* note 55, at 446–47, 462 (recommending phased productions for non-U.S. data to allow time for safeguard implementation, and advising parties to "produce responsive data collected from U.S. custodians first and determine whether further production from non-U.S. custodians is necessary"); Coventry Cap. U.S. LLC v. EEA Life Settlements Inc., No. 17 Civ. 7417 (VM) (SLC), 2020 WL 7383940, at *10 (S.D.N.Y. Dec. 16, 2020) (implementing phased discovery by adding a targeted custodian while excluding others at that stage, requiring search-term testing and a hit report before determining whether broader production was warranted, and providing for meet-and-confer procedures and potential in camera review for sensitive materials).

86. Fed. R. Civ. P. 26(c) (authorizing protective orders governing access, use, and handling of sensitive discovery material).

87. Seattle Times Co., 467 U.S. at 34-35 (explaining that "[b]ecause of the liberality of pretrial discovery permitted by Rule 26(b)(1), it is necessary for the trial court to have the authority to issue protective orders conferred by Rule 26(c)").

copying, downloading, and onward transfer; encryption; deletion or return protocols at the conclusion of the case; field-level redaction of identifiers; and pseudonymization that preserves evidentiary utility while reducing privacy exposure.[88] Courts can also employ Rule 502(d) orders[89] to reduce privilege-related risks that often intensify when cross-border review and production are accelerated. If these robust safeguards are imposed, the incremental risk and burden associated with producing Chinese data would decrease, making narrower, better-protected production a more proportionate outcome than total denial of production.

This calibrated approach can be implemented through a short "protective protocol" that specifies where the data will reside, who may access it, and what uses are permitted. A court might require that China-derived ESI be hosted in a secure review environment with specific audit logging; restrict access to outside counsel and retained experts; prohibit downloading or external transfer absent agreement or further order; and require redaction or pseudonymization of direct identifiers (e.g., national ID numbers, home addresses), unless the requesting party can show that unredacted identifiers are necessary for a specific dispute. Where disagreements persist, courts can validate the adequacy of redactions or sampling through in camera review, (judicial review of materials privately in chambers without disclosure to the opposing party) rather than forcing all-or-nothing production.[90] This kind of calibrated package makes comity operational because it permits disclosure of relevant evidence, while reducing dissemination risk and narrowing exposure to privacy and data security risks to what the case actually requires.

D. Applying the Rubric to Common Discovery Scenarios

The payoff of a proportionality-centered rubric is predictable decision-making in recurring disputes. Two examples illustrate how the framework can produce more consistent outcomes than an ad hoc, "comity-only," approach.

---

88. *See* PIPL arts. 4 (excluding anonymized information from PIPL's scope entirely, thereby eliminating the privacy compliance burden for fully anonymized productions), 51(3) (requiring processors to adopt "security technical measures such as encryption and de-identification" as a baseline compliance obligation); The Sedona Conference, *supra* note 55, at 424–25 (illustrating how pseudonymization and anonymization allow documents to be produced for litigation use while removing or masking direct identifiers, such as national ID numbers, addresses, and phone numbers, to reduce privacy exposure).

89. Fed. R. Evid. 502(d) (authorizing courts to enter orders providing that inadvertent disclosure of privileged material in connection with litigation does not constitute a waiver of privilege in any federal or state proceeding); *see also* Fed. R. Evid. 502 Explanatory note (explaining that Rule 502 "provide a predictable, uniform set of standards under which parties can conduct discovery").

90. U.S. v. Zolin, 491 U.S. 554, 555 (1989) (approving "in camera review" as a means of assessing necessity and scope of disclosure); Astra Aktiebolag v. Andrx Pharms., Inc., 208 F.R.D. 92, 95, 107 (S.D.N.Y. 2002)(conducting in camera review to evaluate privilege assertions, and determine whether redacted or full disclosure was warranted), (both illustrating procedural tools that can be applied in cross-border discovery disputes, including those involving Chinese law)

Scenario 1: Employee email and HR data stored in China (employment or trade secrets case).[91]

A plaintiff seeks broad email and HR files for multiple China-based custodians over several years. Under the rubric, the requesting party must justify why each category is necessary and why narrower sources (U.S.-based custodians, targeted terms, or shorter date ranges) are insufficient. The responding party must identify which data are sensitive (e.g., government IDs, medical info, biometric access logs) and propose minimization alternatives. The court can then order a phased plan: production first from U.S.-based custodians and non-sensitive business communications; then a targeted subset of China-based emails; and only if needed, limited HR materials with redactions and an attorneys'-eyes-only protective order. This approach mirrors proportionality practice in domestic ESI cases, while aligning with PIPL's minimization and necessity constraints.[92]

Scenario 2: Customer or transaction database in China (securities or commercial fraud case).[93]

A party requests full database exports. The rubric encourages field-level minimization: production of only the fields necessary to prove key elements (e.g., transaction timestamps, amounts, internal identifiers), with direct identifiers removed or pseudonymized unless truly needed. If the requesting party later demonstrates that specific identifiers are necessary (for example, to link communications to transactions), the court can order a second phase with a narrower set of identifiers under heightened safeguards. This phased approach reduces cross-border exposure while preserving core evidentiary value and creates a transparent record of necessity if disputes escalate.

Across scenarios, the rubric offers a consistent template for courts to employ: specificity, necessity (achieved through phased discovery), and risk mitigation through calibrated safeguards. However, the framework does not guarantee that every conflict can be solved through balancing. Some disputes implicate provisions, such as restrictions on providing data to foreign judicial or law enforcement authorities, that may require separate analysis and may form the "hard cases" addressed in Part V.[94] But even where limits exist, a proportionality-centered method improves predictability by clarifying what courts will ask parties to show, what mitigation steps matter, and how production can be tailored rather than treated as an all-or-nothing decision.

---

91. *See, e.g.*, Inventus Power, Inc. v. Shenzhen Ace Battery Co., No. 20-CV-3375, 2020 WL 3960451 (N.D. Ill. July 13, 2020) (trade secrets action under the Defend Trade Secrets Act involving allegations that former employees downloaded large volumes of confidential documents before joining a Chinese competitor, generating discovery disputes centered on China-based custodians and electronically stored information)

92. *See* Oxbow Carbon & Mins. LLC v. Union Pac. R.R., 322 F.R.D. 1, 4–10 (D.D.C. 2017) (applying all six Rule 26(b)(1) proportionality factors to compel production of CEO's ESI over respondent's objection that production would be unduly burdensome and disproportionate, finding cost proportionate relative to amount in controversy); PIPL arts. 5–6 (necessity and minimization principles).

93. *See, e.g.,* In re DiDi Glob. Inc. Sec. Litig., No. 21-cv-5807 (LAK), 2025 WL 743964 (S.D.N.Y. Mar. 7, 2025) (securities class action arising from the IPO of a Chinese ride-hailing company, in which discovery disputes involved documents and data stored in China and implicated PRC data-security and cross-border transfer restrictions).

94. *See* PIPL art. 41 (foreign judicial/law enforcement requests for personal information); DSL art. 36 (restrictions on providing data to foreign judicial/law enforcement authorities).

V. Limits and Payoffs of a Proportionality-Centered Approach

A. Structural Limits on Convergence Between Current Rule 26(b)(1) and PIPL

Even with functional convergence, there are structural limits: proportionality can harmonize many conflicts but cannot fully dissolve sovereignty-based constraints or override mandatory rules in either system. Some elements of China's privacy and data-security regime are categorical in form and therefore resist full incorporation into case-by-case proportionality balancing. For example, China's localization rules for certain regulated entities and datasets operate as ex ante territorial controls, rather than discretionary standards. The Cybersecurity Law requires critical information infrastructure operators to store certain personal information and "important data" inside mainland China, allowing cross-border transfer only when necessary and subject to prescribed security procedures.[95] Likewise, China's outbound transfer regime frequently conditions transfers on regulatory mechanisms such as security assessments or standardized contractual filings, which may introduce approvals, sequencing, and timing constraints that litigation-driven proportionality cannot eliminate.[96]

A second category of structural constraint arises when Chinese law regulates both the scope of processing and the recipient and institutional channel of disclosure. The DSL provides that domestic organizations and individuals must receive permission from competent PRC authorities to provide data stored in China to foreign judicial or law-enforcement bodies. In addition, the DSL frames foreign requests for such data as matters to be handled through PRC authorities under treaties, agreements, or reciprocity principles.[97] PIPL contains a similar provision for requests by foreign judicial or law-enforcement authorities for personal information stored domestically in China.[98] These provisions are difficult to absorb into proportionality because they speak in sovereignty terms, including data localization requirements and rules requiring that foreign requests be handled through PRC authorities, rather than in marginal cost-benefit terms.

On the U.S. side, courts remain bound by the Federal Rules' truth-seeking and adjudicatory commitments. *Aérospatiale* instructs courts to resist categorical rules that would automatically require (or forbid) the use of Hague Convention procedures, instead directing a multi-factor comity analysis when foreign law conflicts with U.S. discovery obligations.[99] But the same case also makes clear that comity is not a license to abandon core adjudicatory needs: U.S. courts may compel discovery when the requested evidence

95. Cybersecurity Law of the People's Republic of China art. 37 (requiring certain data localization for critical information infrastructure operators and conditioning cross-border transfers).

96. *See, e.g.,* Outbound Data Transfer Security Assessment Measures (establishing self-assessment plus CAC review mechanisms for certain outbound transfers).

97. DSL art. 36 (requiring that requests by foreign judicial or law-enforcement authorities for data stored in China be handled through competent PRC authorities).

98. PIPL art. 41.

99. Société Nationale Industrielle Aérospatiale, 482 U.S. at 522.

is important, alternatives are ineffective, and the competing interests do not justify withholding.[100] Current Rule 26(b)(1) similarly requires courts to manage scope through proportionality,[101] but it does not permit foreign law to operate as an automatic veto over relevant discovery simply because a party invokes it.[102]

Finally, differences in institutional design matter. China's data governance is enforced substantially through administrative supervision and national-security-oriented regulatory tools, reflected in statutory purpose provisions that expressly prioritize national sovereignty, security, and development interests.[103] U.S. discovery, by contrast, is a court-administered adversarial process designed to develop a factual record for adjudication. Even where the systems appear to share a proportionality-like structure, the interests being balanced, the institutions conducting the balancing, and the consequences of noncompliance can differ in fundamental ways. Proportionality can narrow disputes and discipline judicial discretion through standardization of criteria, but it cannot erase these foundational differences.

B. Hard Cases: State Secrets, National Security, and "National Core Data"

For national-security and core-state-interest data, the proportionality framework primarily clarifies and legitimizes non-disclosure decisions, rather than enabling full reconciliation of U.S. and Chinese demands.[104] China's DSL establishes a categorized and graded data protection system, and identifies "core state data", such as data related to national security, the lifeline of the national economy, major public interests, and important aspects of people's lives, for which a stricter management system applies.[105] The DSL includes review mechanisms for data processing and cross-border transfers of data related to national security, and it recognizes that secrecy law applies where data handling involves state secrets.[106] In such cases, the conflict is not merely that production is burdensome or risky; rather, the legal regime itself treats disclosure as incompatible with core security interests.

These are "hard cases" because many of the mitigation strategies[107] that make proportionality productive elsewhere may be insufficient if the information is classified or deemed security-sensitive at the level of state interests.[108]

---

100. *Id.*

101. Fed. R. Civ. P. 26(b)(1).

102. *See* Société Nationale Industrielle Aérospatiale, 482 U.S. at 542-44 (rejecting a blanket rule requiring deference to foreign procedures and holding that courts must conduct a particularized, case-specific comity analysis rather than treat foreign law as dispositive).

103. DSL art. 1 (stating purposes including safeguarding national sovereignty, security, and development interests).

104. DSL arts. 21, 24, 53.

105. *Id.* art. 21 (creating categorized and hierarchical protection, and providing that certain data constitute "core state data" subject to stricter management).

106. *Id.* arts. 24 (national security reviews; decisions final), 53 (state secrets law applies where data handling involves state secrets).

107. Mitigation strategies, such as redaction, pseudonymization, protective orders, staged production, and in-country review.

108. U.S. v. Reynolds, 345 U.S. 1, 10-11 (1953) (holding that a formal claim of privilege supported by a reasonable danger that disclosure would expose military secrets is sufficient

Protective measures can reduce dissemination risk, but they cannot authorize disclosure of information that the producing party is legally prohibited from sharing. Recent revisions to China's secrecy framework, which broadened and tightened secrecy obligations, reinforce this point: the compliance risk is not purely theoretical, and it is not always reducible through private ordering between litigants.[109]

U.S. law contains analogous "hard limits" to override proportionality and foreclose disclosure altogether. In civil litigation, the state secrets privilege, a common-law evidentiary privilege recognized in *United States v. Reynolds*, can require dismissal or foreclose discovery where disclosure would threaten national security.[110] The court in *Reynolds* formalized the privilege, and emphasized that courts must assess such claims in a manner that avoids compromising the security interests the privilege is meant to protect.[111] In criminal cases, Congress adopted the Classified Information Procedures Act (CIPA) to provide procedures for managing classified information, including mandatory protective orders upon government motion, again reflecting that some information cannot simply be "balanced into" ordinary disclosure rules.[112] The similarity is not that Chinese and U.S. national security laws are identical, but that both systems recognize zones where ordinary disclosure norms yield to categorical security constraints. In those domains, proportionality can still play a valuable role by clarifying what is genuinely off-limits for discovery purposes and ensuring courts exhaust narrower substitutes first. However, proportionality cannot supply an evidentiary substitute when the law treats disclosure as non-negotiable.

C. Normative Payoffs: Why Proportionality Still Matters for Transnational Discovery

Even if proportionality cannot solve every hard case, it offers substantial benefits, such as greater coherence, predictability, and legitimacy, that make transnational discovery more manageable and normatively defensible. First, a proportionality-centered approach improves doctrinal coherence. By integrating PIPL- and DSL-related burdens into Current Rule 26(b)(1)'s existing balancing structure, courts can avoid oscillating between extremes and instead evaluate objections through principles already embedded in federal procedure. The Advisory Committee's 2015 amendments and notes reflect this institutional expectation: proportionality is not a special doctrine reserved for unusual cases, but a baseline principle that courts and

---

to bar compelled production); *see also* DSL art. 31 (imposing heightened restrictions on processing and transfer of "important data" tied to national security).

109. Feifei Ren & John Davis, *China's Revised and More Stringent State Secrets Law Takes Effect*, Reuters (May 7, 2024), https://www.reuters.com/legal/legalindustry/chinas-revised-more-stringent-state-secrets-law-takes-effect-2024-05-07[https://perma.cc/86VS-55LY].

110. U.S. v. Reynolds, 345 U.S. 1, 10–11 (1953)

111. *Id.*

112. Classified Information Procedures Act, Pub. L. No. 96–456, 94 Stat. 2025 (1980) (codified as amended at 18 U.S.C. app. III); *see also* Cong. Rsch. Serv., The Classified Information Procedures Act (CIPA) (Nov. 6, 2024).

parties share responsibility to apply, and it is not satisfied by boilerplate objections.[113]

Second, proportionality increases predictability and encourages ex ante planning. A clear rubric gives parties guidance on what courts will ask them to show (necessity, alternatives tried, and proposed safeguards), which in turn improves negotiation, reduces motion practice, and makes discovery timelines more realistic where China-based data is implicated.[114] This is especially valuable when cross-border transfer mechanisms require sequencing and compliance steps that do not map neatly onto U.S. discovery schedules. Even when a party ultimately must seek relief through treaty channels or government approvals, ex ante proportionality analysis at the outset of discovery planning can narrow what must be pursued through those channels.

Third, proportionality can enhance legitimacy and reciprocity. When courts acknowledge foreign privacy and data regimes as relevant to burden and risk—rather than dismissing them as tactical noise—they reduce the perception that U.S. discovery is indifferent to sovereignty and privacy concerns. That posture does not guarantee compliance or cooperation, but it supports more principled adjudication and can reduce incentives for parties to deploy foreign law as a blunt shield.

Finally, proportionality creates better incentives for litigants. It rewards parties who design discovery plans around minimization, phasing, in-country review, and calibrated protective measures—the same techniques corporate actors already use to manage cross-border conflicts in practice. Even when hard cases arise, the proportionality lens forces earlier identification of what is truly necessary, what can be substituted, and what is categorically unavailable. As a result, judicial decisions will be more transparent, and disputes will be more efficiently resolved.

Conclusion

Cross-border discovery disputes involving Chinese data are often framed as an unavoidable clash between expansive U.S. disclosure obligations and restrictive Chinese privacy and data-security laws. This Note has argued that that framing is incomplete. Although the United States and China regulate information access through different legal traditions and institutional structures, both systems now rely on proportionality-based limitation principles to govern when, how, and to what extent information may be accessed. Current Rule 26(b)(1)'s proportionality framework and the PIPL's necessity- and minimization-based regime perform parallel gatekeeping functions, even as they pursue distinct normative goals.

Recognizing this functional convergence does not eliminate sovereignty conflicts or resolve hard cases involving national security, state secrets, or categorical transfer restrictions. But it does offer courts a more coherent and

113. Fed. R. Civ. P. 26(b)(1) advisory committee's note to 2015 amendment.

114. Sedona Conference, *supra* note 55 (endorsing structured planning, in-country collection/review, and limiting production of protected data).

predictable way to manage many transnational discovery disputes. By treating Chinese privacy and data-security obligations as analytically relevant inputs to proportionality—rather than as either dispositive barriers or mere litigation tactics—courts can regulate discovery scope, incentivize early narrowing, and reduce unnecessary cross-border data transfers, without abandoning core adjudicatory commitments.

A proportionality-centered approach also aligns judicial doctrine with existing litigation practice. As courts and corporate actors increasingly rely on minimization, phased production, in-country review, and calibrated protective orders, formalizing these techniques within a unified analytical rubric can improve transparency, predictability, and legitimacy in transnational litigation. In an era of data nationalism and globalized disputes, proportionality provides not a perfect solution, but a shared legal language through which competing systems can be managed rather than allowed to collide.