wgs

The Sedona Conference

Commentary on Proportionality in Cross-Border Discovery

A Project of The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6)

June 2024
Public Comment Version
Submit comments by August 28, 2024,
to comments@sedonaconference.org

Commentary on Proportionality in Cross-Border Discovery

A Project of The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6)

JUNE 2024 PUBLIC COMMENT VERSION

Author: The Sedona Conference

Editors-in-Chief

Briordy Meyers
Jay Yelton III

Contributing Editors

Jim Calvert
William Marsillo
Hon. Xavier Rodriguez
Joshua Samra
Anna-Patricia Stadler
Jeane A. Thomas
Bijal V. Vakil
Michael C. Zogby

Steering Committee Liaison

Nichole Sterling

Staff Editors

David Lumia
Michael Pomarico

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

Preface

Welcome to the public comment version of The Sedona Conference's *Commentary on Proportionality in Cross-Border Discovery* ("*Commentary*"), a project of The Sedona Conference Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law.

The mission of The Sedona Conference is to move the law forward in a reasoned and just way. The mission of WG6 is to develop principles, guidance and best practice recommendations for information governance, discovery, and disclosure involving cross-border data transfers related to civil litigation, dispute resolution and internal and civil regulatory investigations.

The Sedona Conference acknowledges Editors-in-Chief Briordy Meyers and Jay Yelton for their leadership and commitment to the project. We also thank contributing editors Jim Calvert, Bill Marsillo, Judge Xavier Rodriguez, Joshua Samra, Anna-Patricia Stadler, Jeane Thomas, Bijal Vakil, and Michael Zogby for their efforts. We thank Nichole Sterling for her contributions as Steering Committee liaison to the project. We also thank Elizabeth Holland for her contributions.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG6 who reviewed, commented on, and proposed edits to early drafts of the *Commentary* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG6 meetings where drafts of this *Commentary* were the subject of dialogue. On behalf of The Sedona Conference, I thank all of them for their contributions.

Please note that this version of the *Commentary* is open for public comment, and suggestions for improvement are welcome. Please submit comments by August 28, 2024, to comments@sedonaconference.org. The editors will review the public comments and determine what edits are appropriate for the final version.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG6 and several other Working Groups in the areas of electronic document management and discovery, data security and privacy liability, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Kenneth J. Withers
Deputy Executive Director
The Sedona Conference
June 2024

Table of Contents

I. INTRODUCTION

Cross-border discovery is often challenging for parties, practitioners, and courts trying to navigate conflicts between U.S. discovery obligations and non-U.S. laws. Such conflicts are especially prevalent with respect to non-U.S. data protection laws[1]—the type of conflict most directly considered in this *Commentary*—but may include any non-U.S. law that impacts the scope and practice of data preservation and discovery. Although conflicts arising from non-U.S. data protection laws are certainly not new, the challenges and potential burdens have been exacerbated in recent years because of the emergence of new and more stringent data protection laws, evolution in existing data protection regimes, ever-increasing data volumes, and the proliferation of novel communication and collaboration technologies that use and rely on the personal information of the participating users and others.[2]

Along a similar trajectory and driven in part by increasing volumes and types of data subject to discovery, proportionality has increasingly become established as a fundamental principle affecting and limiting the scope of discovery under Federal Rule of Civil Procedure 26(b)(1). While U.S. courts have analyzed the effect of U.S. data privacy laws on the production of documents and information in U.S. litigation, courts typically have not resolved conflicts between U.S. discovery obligations and non-U.S. data protection laws through a proportionality lens. Instead, courts most often have relied on the comity analysis outlined in *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*[3] when considering such conflicts.

Although proportionality and comity are different legal analyses with different goals, they share overlapping factors that may, in some cases lead to identical results whether a court applies one or the other. This *Commentary* examines the landscape of overlapping analyses, offering summaries and commentary on various approaches before recommending a framework that starts with proportionality as a first step—as a threshold issue of discovery scope—while recognizing that proper proportionality analysis may consider the effect of compliance with the non-U.S. law at issue. If the discovery is proportional to the needs of the case, when so considered, *then* a separate comity analysis should be conducted. Although those analyses share similar factors, applying them in strict order should minimize analytic and doctrinal problems.

This *Commentary* also examines the potential costs and burdens of cross-border discovery, including nonmonetary risks and burdens associated with measures implemented to comply with non-U.S. laws, and advises that arguments based on such burdens should be made with sufficient specificity

---

1 As used throughout this *Commentary*, "non-U.S. data protection laws" refers to both privacy and data protection laws and regulations.

2 *See, e.g.*, The Sedona Conference, *International Litigation Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)* vi–viii (2017) [hereinafter *International Litigation Principles*], *available at* https://thesedonaconference.org/publication/International_Litigation_Principles (discussing Sedona's history of analyzing and providing guidance on cross-border discovery challenges).

3 482 U.S. 522 (1987).

and detail. Further, parties and courts should employ and encourage practices that promote compliance with the non-U.S. laws while reducing burdens of cross-border discovery.

II. SCOPE OF U.S. DISCOVERY AND PROPORTIONALITY

In tracking the development of scope in U.S. discovery law, the common themes of technological advances and deploying the Federal Rules of Civil Procedure to gain a competitive advantage frame the story of proportionality.[4] As technology drove the generation and copying of accelerated volumes of documents or objects for discovery, U.S. attorneys developed their focus on discovery rules and honed arguments for leveraging those rules. If one was requesting documents, the focus was on relevance and possibly burdening one's opponent, and if one was responding to document requests, the focus would likely be on arguments and objections around disproportionate burden and protection of privileges or privacy.[5] This in turn put pressure on courts to resolve increasingly rancorous discovery disputes among the parties and decide what was proportional to the needs of the case long before the 1983 and 2015 Amendments to the Rules,[6] whether they used the specific word "proportional" or not.[7] The result has been a slow march toward the realization that cooperation between attorneys committed to a proportional approach to discovery along with hands-on judicial management are what is truly necessary for addressing the challenge of discovery volume and legal gamesmanship.[8]

Importantly, cooperation in the context of those pursuing a reasoned approach to proportionality in discovery scope determinations has increasingly included consideration of nonmonetary challenges unique to parties seeking or providing discovery generated, processed, or stored in non-U.S. jurisdictions. These challenges include immeasurable business disruption and potential reputational risk, navigating protection of various privileges under disparate disclosure and legal privilege standards,[9]

---

4 As an example of how developments in information-related technology and the Federal Rules of Civil Procedure often parallel each other, consider that photocopying was developed in the same year, 1938, that the Federal Rules of Civil Procedure became effective.

5 Early debates around discovery and the Federal Rules of Civil Procedure often framed the privilege protection specifically within the concept of privacy protections for the practicing attorney. *See* Hickman v. Taylor, 329 U.S. 495, 512 (1947) ("[P]rivacy of an attorney's course of preparation is so well recognized and so essential to an orderly working of our system of legal procedure that a burden rests on the one who would invade that privacy to establish adequate reasons to justify production through a subpoena or court order.").

6 Hon. Elizabeth D. Laporte & Jonathan M. Redgrave, *A Practical Guide to Achieving Proportionality Under Federal Rule of Civil Procedure 26*, 9 FED. CTS. L. REV. 20, 24 (2015) ("The doctrine of proportionality has always been available to courts to limit discovery to that which is relevant and necessary for effective litigation of the issues in a case." Authors also point out that Rule 1 itself and its focus on "just," "speedy" and "inexpensive" resolution of disputes has been in place since 1937.).

7 *Hickman*, 329 U.S. at 507 ("[D]iscovery, like all matters of procedure, has ultimate and necessary boundaries."); *id.* at 508 ("[A]s Rule 26(b) provides, further limitations come into existence when the inquiry touches upon the irrelevant or encroaches upon the recognized domains of privilege.").

8 Hon. Craig B. Shaffer, *The "Burdens" of Applying Proportionality*, 16 SEDONA CONF. J. 55, 57 (2015).

9 The Sedona Conference, *Commentary on Cross-Border Privilege Issues*, 23 SEDONA CONF. J. 475 (2022) [hereinafter *Commentary on Cross-Border Privilege Issues*].

and adherence to local or varied data privacy and protection laws.[10] The Sedona Conference, like Rule 26, recognizes noncost factors in determining discovery scope and has consistently advocated for their consideration.[11] Moreover, the specific and common nonmonetary challenges consistently present in cross-border discovery provide another dimension to proportionality analyses in U.S. courts given the accelerated volume of data generation, global business expansion, and the burgeoning global data privacy and protection legal landscape.[12]

In turn, these concurrent forces—rapidly increasing discovery volumes and formats coupled with heightened regulatory and legal scrutiny and obligations around data privacy and protection—are making cross-border discovery especially complex and expensive.[13] While it may be true that the dual burdens of compliance with U.S. discovery rules and non-U.S. privacy and data protection regulation is part of the cost of doing business abroad, it is also true that many organizations have their data hosted, transferred, and used around the globe simply as a result of today's global digital economy. One would be hard-pressed to find any party whose information is not somehow involved in cross-border data flows. This alone is a novel and recent development in the context of U.S. discovery law, but the heightened focus on territorial "digital sovereignty" over the last few years has meant the vector for monetary costs associated with cross-border discovery is likely to continue pointing upward for requesting and responding parties.[14]

There are more data sources than ever before, and they are becoming more complex and dynamic every day. Proportionality considerations in this context should be based on cooperative understandings of data management serving the interests of *both* the requesting and responding parties as an expression of state-of-the-art comprehension of global technologies. Just because there are more data sources does not mean the data itself is proportional to the needs of the case. The unique value of

---

[10] The Sedona Conference, *Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders*, 21 SEDONA CONF. J. 393 (2020); see also The Sedona Conference, *Commentary on the Enforceability in U.S. Courts of Orders and Judgments Entered Under GDPR*, 22 SEDONA CONF. J. 277 (2021); The Sedona Conference, *Commentary on Managing International Legal Holds*, 24 SEDONA CONF. J. 161 (2023) [hereinafter *Commentary on Managing International Legal Holds*].

[11] *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 68 (2018) (Comment 2.d., addressing Sedona Principle 2, states that "[p]arties should address the full range of costs of preserving, collecting, processing, reviewing, and producing ESI"); *id.* at 69 ("[T]he non-monetary costs (such as the invasion of privacy rights, risks to business and legal confidences, and the risks to privileges) should be considered.").

[12] *See International Litigation Principles*, *supra* note 2.

[13] Michael Baylson, *Cross Border Discovery at a Crossroads*, 100 JUDICATURE 56 (2021); see also Atif Khawaja, *INSIGHT: Discovery Process, Costs Can Confuse Foreign Companies Caught in U.S. Litigation*, BLOOMBERG LAW (Mar. 12, 2019), https://news.bloomberglaw.com/us-law-week/insight-discovery-process-costs-can-confuse-foreign-companies-caught-in-u-s-litigation.

[14] David McCabe & Adam Satariano, *The Era of Borderless Data is Ending*, N.Y. TIMES (May 23, 2022), https://www.nytimes.com/2022/05/23/technology/data-privacy-laws.html.

the data in the cross-border discovery context is especially important, and the shared goal should be to surgically provide what is actually necessary.

A. U.S. Discovery Pre-2015

1937: Birth of the Federal Rules of Civil Procedure and Broad Discovery

Although explicit references to proportionality in the Rules would not come until 1983, the history of courts working to manage debates around the scope and burdens of discovery predates the Rules themselves. The Notes of the Advisory Committee on Rules-1937, in discussing what would become the entirely new Rule 26(b) regarding the scope of depositions, stated that "while the old chancery practice limited discovery to facts supporting the case of the party seeking it, this limitation has been largely abandoned by modern legislation," citing multiple state codes of civil procedure as support for the trend of broadening the discovery scope in U.S. federal courts beyond just facts to support one's own case.[15] Both courts and academics interpreting the new Rules noted the ushering in of an era of more liberal discovery,[16] abolishing the procedural distinctions between law and equity and evidentiary versus ultimate or material facts, converting the burdens of pleading to crystallize issues and reveal facts to simply notice-based pleading,[17] and removing the restrictions on obtaining discovery only within the exclusive knowledge or control of the adverse party. They have also interpreted these Rules as providing new allowances for discovery into not only one's own case but the facts underpinning the adverse party's case.

An example of the recognition of this shift can be seen in *Nichols v. Sanborn Co.*, an equity patent-infringement suit involving electrocardiograph device patents. [18] The plaintiffs, via interrogatories, sought information about diagrams, literature, and designs for the electrocardiographs at issue from the defendant manufacturer, and the defendant objected on the grounds of Equity Rule 58 that the interrogatories focused on evidentiary details instead of the requisite facts—lodging the familiar complaint about plaintiffs being on a "fishing expedition."[19] The court overruled the defendant's objections based on the new Rules, which allowed for discovery into both the opposing party's case and facts in their possession, explaining that "to keep in step with the purpose and spirit underlying the adoption of these rules it is better that liberality rather than restriction of interpretation be the guiding principle."[20]

---

15 FED. R. CIV. P. 26(b) advisory committee's note to 1937 rule.

16 Alexander Holtzoff, *Instruments of Discovery under Federal Rules of Civil Procedure,* 41 MICH. L. REV. 205, 205 (1942) ("Broad and liberal discovery is one of the outstanding contributions to civil procedure made by the new federal rule . . . [a] veritable arsenal of weapons for discovery is provided, from which a skilled lawyer may select those best suited for this purpose, just as an experienced golfer chooses the club which fits his immediate needs.").

17 James A. Pike & John W. Willis, *Federal Discovery in Operation*, 7 UNIV. OF CHICAGO L. REV. 297, 297 (1940).

18 Nichols v. Sanborn Co., 24 F. Supp. 908, 910 (D. Mass. 1938) (cited by Holtzoff, *supra* note 16, at 207).

19 *Id.* at 909–10.

20 *Id.* at 911.

Rule 34 required that a party seeking inspection or discovery of documents or tangible objects first show good cause, specifically naming the objects of discovery in another party's possession or control via motion practice, and then be granted a court order before moving forward with such discovery. Courts interpreting Rule 34 debated whether it should be restricted to only admissible evidence given the broad scope for deposition discovery in Rule 26, which was not so limited. Some judges held that Rule 34 could not have been meant to be limited to admissible evidence, while others insisted that the rules be read separately.[21]

The major takeaway from these debates is that arguments about what exactly was within scope for discovery and how the rules could or should be read together to carry out discovery by leveraging them strategically is neither new nor unique to twenty-first century discovery. Instead, the hope was that the new Rules would end complaints of "fishing expeditions" both because the scope of discovery was now broad enough to allow for some fishing and the structure of the rules organized enough to keep the fisherman focused only on fish that mattered.[22]

1946 Amendment: Reasonably Calculated to Lead to the Discovery of Admissible Evidence

The 1946 amendment to Rule 26(b) added the "reasonably calculated to lead to the discovery of admissible evidence" language, continuing the explicit broadening of U.S. discovery and notching another important contribution in the march toward the proportionality standard.[23] The Notes of the Advisory Committee on Rules-1946 in discussing the amendment state that "the purpose of discovery is to allow a broad search for facts," and that the amendment makes "clear the broad scope of examination and that it may cover not only evidence for use at the trial but also inquiry into matters in themselves inadmissible as evidence but which will lead to the discovery of such evidence." However, this broad scope does have a limit, as "matters entirely without bearing either as direct evidence or as leads to evidence are not within the scope of inquiry."[24] The Advisory Committee explained that the amendment was needed specifically because courts were still erroneously applying an admissibility standard when limiting the scope of discovery through deposition testimony. Rule 34 was also amended from "evidence material to any matter involved in the action" to "evidence relating to any of the matters within the scope of the examination permitted by Rule 26(b)" in a purposeful attempt to address the potential confusion around differing scopes for depositions and discovery of documents and things for inspection.[25]

---

21 Holtzoff, *supra* note 16, at 221.

22 Pike & Willis, *supra* note 17, at 301; Holtzoff, *supra* note 16, at 205; *Nichols*, 24 F. Supp. at 507.

23 FED. R. CIV. P. 26(b) (1948) (modified 1970). Language added to Rule 26(b): "It is not ground for objection that the testimony will be inadmissible at the trial if the testimony sought appears reasonably calculated to lead to the discovery of admissible evidence."

24 FED. R. CIV. P. 26(b) advisory committee's note to 1946 amendment.

25 FED. R. CIV. P. 34 advisory committee's note to 1946 amendment.

1970 Amendment: Further Broadening of Discovery

The 1970 amendment to Rule 26(b) may be one of the most important in the march toward proportionality because it moved the broad scope outside the limits of deposition testimony "to cover the scope of discovery generally," and made clear that "all provisions as to scope of discovery are subject to the initial qualification that the court may limit discovery in accordance with these rules," including incorporation by reference to Rules 33 and 34.[26] Importantly, Rule 34 was also amended, this time removing the good-cause requirement, which had caused confusion and inconsistent interpretations, and allowing for extrajudicial discovery of documents and things.[27] Together, these amendments handed over to counsel the responsibility for making and responding to document requests while trying to apply a consistent scope definition for both deposition and document-based discovery, which had now started to include electronic data compilations.[28]

1980 Amendment: Discovery Conferences

While the 1970 amendments to Rules 26 and 34 attempted to provide a consistent definition of discovery scope and allow counsel to request and produce documents without the micromanagement of courts, by 1976, abuse of the discovery process had gotten so bad that an American Bar Association (ABA) task force was established to address "unfair use of the discovery process."[29] Although the Rule 26(f) conference was added in 1980 to help address "widespread criticism of abuse of discovery," the Advisory Committee on Rules explained that it perceived the problem to be severe in limited cases rather than a general issue requiring application of considered amendments to Rule 26(b)(1).[30] Rule 34(b) was amended to add that a "party who produces documents for inspection shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the request," with the Advisory Committee noting the ABA task force's report, stating, "it is apparently not rare for parties deliberately to mix critical documents with others in the hope of obscuring significance."[31] But some practitioners felt the 1980 amendments did not go far enough in providing a framework for properly addressing discovery abuses and the problems associated with disproportionate application or leveraging of the rules for advantage in litigation.[32]

---

[26] FED. R. CIV. P. 26(b) advisory committee's note to 1970 amendment.

[27] FED. R. CIV. P. 34 advisory committee's note to 1970 amendment.

[28] *Id.*

[29] Laporte & Redgrave, *supra* note 6, at 25.

[30] FED. R. CIV. P. 26 advisory committee's note to 1980 amendment.

[31] FED. R. CIV. P. 34 advisory committee's note to 1980 rule. ("*Subdivision (b).* The Committee is advised that, 'It is apparently not rare for parties deliberately to mix critical documents with others in the hope of obscuring significance.' *Report of the Special Committee for the Study of Discovery Abuse, Section of Litigation of the American Bar Associated* (1977) 22. The sentence added by this subdivision follows the recommendation of the *Report*.").

[32] Laporte & Redgrave, *supra* note 6, at 26.

1983 Amendments: Proportionality's Implicit Arrival

By 1983 it had become apparent that reliance on the parties and Rule 26(f) conferences to curb discovery abuses was not sufficient and that the everlasting problem of "fishing expeditions" in the beautiful waters of broad discovery had only gotten worse over time as attorneys leveraged the rules for tactical advantage instead of honoring the spirit of the rules.[33] Some might argue that the pre-1983 language in Rule 26(a), which provided for no limit on the frequency and use of depositions, interrogatories, document productions and requests for admissions, simply invited the very gamesmanship the rules were attempting to control for in 1937. The 1983 amendments to Rule 26 were a direct reaction to "over-discovery"[34] by: removing the unlimited language from Rule 26(a), changing the heading of Rule 26(b) from "Scope of Discovery" to "Discovery Scope and Limits," and most importantly, detailing the criteria for those limitations in Rule 26(b)(1).

The amendment to Rule 26(b)(1) included a new paragraph that for many attorneys represents the "formal" embedding of the concept of proportionality language in the Rules:[35]

> The frequency or extent of use of the discovery methods set forth in subdivision (a) shall be limited by the court if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the discovery is unduly burdensome or expensive, taking into account the needs of the case, the amount in controversy, limitations on the parties' resources, and the importance of the issues at stake in the litigation. The court may act upon its own initiative after reasonable notice or pursuant to a motion under subdivision (c).

Although the literal use of "proportional" or "proportionality" was not included in the 1983 amendments, it was clear from the advisory committee's notes that instilling a proportional approach to discovery that included nonmonetary factors such as free speech, employment issues, and public policy, was the goal.[36] It also was clear that the intent was to include and give weight to

---

[33] FED. R. CIV. P. 26 advisory committee's note to 1983 amendment. The committee noted multiple studies detailing the issues with either excessive discovery requests or avoidance of reasonable discovery requests and the resulting costs in time and expenses "disproportionate to the nature of the case, the amount involved, or the issues or values at stake."

[34] *Id.*

[35] Laporte & Redgrave, *supra* note 6, at 22.

[36] "Thus the rule recognizes that many cases in public policy spheres, such as employment practices, free speech, and other matters, may have importance far beyond the monetary amount involved. The court must apply the standards in an even-handed manner that will prevent use of discovery to wage a war of attrition or as a device to coerce a party, whether financially weak or affluent." FED. R. CIV. P. 26 advisory committee's note to 1983 amendment; *see also* Shaffer, *supra* note 8, at 62–63 (noting that "the 1983 change to Rule 26(b)(1) sought to instill a more

nonmonetary factors that might be unique to an individual party and touch on nonlegal issues complicating discovery but nevertheless remained important in the overall balancing test.

The 1983 amendments also included the creation of Rule 26(g), which gave teeth to the requirement that discovery be properly limited by requiring attorneys requesting discovery or responding to discovery requests to certify that they had conducted a "reasonable inquiry" that said discovery request or response was "consistent with the rules," "not interposed for any improper purpose, such as to harass or to cause unnecessary delay or needless increase in the cost of litigation," and "not unreasonable or unduly burdensome" given the specific factors outlined in Rule 26(b)(1)(iii). While not explicit, the amendments solidified a proportional approach to discovery through not only the edits and additions to scope language but also the provision of sanctions for failing to take a proportional approach to discovery and leveraging it beyond the needs of the case.[37]

1993 Amendments: Maybe Two More Factors Will Help (Or Hurt?)

As discovery moved into the 1990s, however, it appeared as if the teeth of the 1983 amendments provided very little bite for litigants and courts, as the purpose of the Rules was largely ignored. Counsel did not consistently apply the amendments, and there is little case law to demonstrate enforcement of proportionality concepts embedded in Rule 26(g), despite the explosion of ESI throughout the 1990s.[38] One notable exception is *In re Convergent Technologies Securities Litigation*,[39] in which Magistrate Judge Wayne D. Brazil drafted an opinion that represents a master class summary of the proper application of the proportionality principles, the intent of the Rule 26 advisory committee's amendments, and the aggregate negative impact on the practice of law caused by attorneys leveraging discovery as a weapon, as they did in this case—to the tune of a $40,000 dispute over *when* interrogatories should be answered.

As a result of too many discovery disputes and too few opinions like *In Re Convergent*, the rules committee again revised Rule 26(b) in 1993, adding two additional factors: "burden or expense of the proposed discovery outweighs its likely benefit" and "importance of the proposed discovery in resolving this dispute," noting that the textual changes were made "to enable the court to keep tighter rein on the extent of discovery" and to "provide the court with broader discretion to impose additional restrictions on the scope and extent of discovery."[40] However, and perhaps most importantly, the amendments also moved the implicit proportionality factors outside the sub-section defining the

proportionate approach to discovery, while still respecting the parties' right to 'discovery that is reasonably necessary to afford a fair opportunity to develop and prepare the case.'") (citing Leksi, Inc. v. Fed. Ins. Co., 129 F.R.D. 99, 103 (D.N.J. 1989)).

37 Shaffer, *supra* note 8, at 63 ("The 1983 amendments also sought to advance the goal of proportionality with a new Rule 26(g)."); Laporte & Redgrave, *supra* note 6, at 28 ("As is clear from the text, 26(g)(1)(B) tracked the notions of proportionality reflected in Rule 1 and the contemporaneously added Rule 26(b)(1).").

38 Laporte & Redgrave, *supra* note 6, at 29.

39 108 F.R.D. 328, 331 (N.D. Cal. 1985).

40 FED. R. CIV. P. 26 advisory committee's note to 1983 amendment.

scope of discovery and may have unintentionally muddied the waters of discovery fishing expeditions even further.

Despite—or arguably because of—the 1993 Amendments provision of two additional proportionality factors and stated intent of directly addressing over-discovery head on, "its effect on discovery practice appear[ed] to have been muted."[41]

B. 2015 Amendments: Explicit Proportionality

As the 1990s saw the explosion of data and the ongoing failure of the bar to apply principles of proportionality to discovery practice properly, the 2006 Advisory Committee on Rules again stepped in with a revision to Rule 26(b)(2) adding the "not reasonably accessible" language, followed by more tweaks in 2007 to Rule 26(b)(1) to emphasize the limits of discovery scope.

Yet the seismic shift came with the 2015 amendments and the 2015 Advisory Committee on Rules' explicit placement of both the word and concept of proportionality in the Rules by changing the language of Rule 26(b)(1) to what we have today: an equal apportionment of relevance and proportional value embedded into the definition of scope.

(b) Discovery Scope and Limits.

Rule 26(b)(1) provides:

> (1) *Scope in General.* Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

The 2015 Committee Note explained that revising 26(b)(1) intended to bring proportionality back to its rightful place, the place the 1983 amendments originally had it. The "reasonably calculated" language was also removed as it was leveraged by some practitioners to define the scope of discovery improperly. The 2015 amendment did not "change the existing responsibilities of the court and the parties to consider proportionality" nor "place on the party seeking discovery the burden of addressing all proportionality considerations" but was meant to emphasize that the "parties and the court have a collective responsibility to consider the proportionality of all discovery and consider it in

[41] Laporte & Redgrave, *supra* note 6, at 29.

resolving discovery disputes"—a responsibility that for the attorneys is reinforced by their Rule 26(g) obligations.

The 2015 Committee Note also emphasized that proportionality considerations are not—and had not been in the past—simply limited to monetary factors:

> It also is important to repeat the caution that the monetary stakes are only one factor, to be balanced against other factors. The 1983 Committee Note recognized "the significance of the substantive issues, as measured in philosophic, social, or institutional terms. Thus the rule recognizes that many cases in public policy spheres, such as employment practices, free speech, and other matters, may have importance far beyond the monetary amount involved." Many other substantive areas also may involve litigation that seeks relatively small amounts of money, or no money at all, but that seeks to vindicate vitally important personal or public values.

Although the proportionality language was the star of these amendments, Rule 26(b)(2)(C)(iii) was also amended to add "must" language obligations on the court as the discovery case manager. Not only did proportionality and relevancy work in concert to define scope, but courts were now obligated to ensure discovery requests and responses maintained both elements and not only *should* but *must* act when they spot disproportionate discovery:

> (C) *When Required.* On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:
>
> (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;
>
> (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or
>
> (iii) the proposed discovery is outside the scope permitted by Rule 26(b)(1).

The 2015 Committee Note held attorneys responsible as well, reminding everyone that it is still up to the advocates to concretely establish all elements of the proportional scope definition with specificity if they wanted their argument to win.

Two days after the December 1, 2015, effective date of the Rule 26(b)(1) amendments, U.S. Magistrate Judge James C. Francis interpreted the new proportionality rule in *State Farm Mutual Automobile*

Insurance Co. v. Yuri Fayda.[42] While State Farm was seeking the bank records and tax returns of an individual defendant, a subset group of defendants objected based on relevancy and privacy. Judge Francis quoted the 2015 Committee Notes, which made clear that the amendments were "intended to 'encourage judges to be more aggressive in identifying and discouraging discovery overuse' by emphasizing the need to analyze proportionality before ordering production of relevant information." In the context of his proportionality and relevancy analysis around the tax records, Judge Francis stated that federal courts often consider objections to discovery based on privacy rights. The problem was that the defendant did not articulate privacy as a proportional burden, leading the court to grant the motion to compel production of the tax records. Importantly, Judge Francis noted, the amendments did not change the burdens of the parties in terms of establishing relevancy or undue burden or expense. The party seeking discovery has the burden of relevancy, the party resisting discovery has the burden of showing undue burden or expense, and as the Committee Note stated, the amendment "does not place on the party seeking discovery the burden of addressing all proportionality considerations" on its own.[43]

State Farm is notable not just for its timing but because it was a harbinger of what was to come: continued acceleration of volumes, types, and formats of Electronically Stored Information (ESI), coupled with rising data privacy and protection scrutiny and the continued frustration of courts with the failure of parties to follow the lead of the amendments to the Rules[44] and The Sedona Conference's Principles of Proportionality by actually articulating the burden with specific information.[45]

C. Post-2015: Grappling for a Matrix in a Cross-Border World

In the context of cross-border discovery, what is most important to remember about U.S. law is that it has consistently adjusted its approach to scope and proportionality to the challenges of the time. Perhaps for some practitioners the adjustments were not timely, correct, or comprehensive, but they were repeatedly driven by the contemporary dynamics of technology and attorney practice trends. In reviewing the above history, there is a clear pattern in the scope of amendments to the Rules being driven by a single question: How can we allow fair and broad discovery while focusing requesting

---

[42] State Farm Mut. Auto. Ins. Co. v. Fayda, No. 14 Civ. 9792 (WHP) (JCF), 2015 WL 7871037 (S.D.N.Y. Dec. 3, 2015).

[43] *Id.* at *2–4.

[44] Fifty-two percent of federal judges replied that parties should use metrics when asked "What can lawyers do to improve proportionality arguments," EXTERRO, 2018 ANNUAL FEDERAL JUDGE'S SURVEY; Eighty-three percent of federal judges replied that working together without the court to identify reasonable and proportionate eDiscovery parameters when asked "What do you consider the important components of cooperation," EXTERRO, 2019 ANNUAL FEDERAL JUDGE'S SURVEY; One hundred percent of federal judges answered "True" to the statement "With more effective eDiscovery processes and a greater willingness to cooperate, parties would reduce costs and not sacrifice defensibility," and 84 percent said "Yes" when asked "Would you like to see parties leverage the concept of proportionality more often when defining eDiscovery parameters," EXTERRO, 2020 ANNUAL FEDERAL JUDGE'S SURVEY.

[45] The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141 (2017).

and responding parties on only what is needed for the present matter before the court, help (if not prompt) the court to proactively manage its docket, and ultimately ensure that discovery does not derail the "just, speedy, and inexpensive determination of every action and proceeding"?[46]

When the Rules were first established, they promised a reasonable opportunity for opening up discovery. There were not as many documents back then and the challenge was developing any set of evidence-based facts given the demands around pleadings and restrictions on discovery at the time. After printing took off, computers accelerated the volume and complexity of discoverable information. The evolution of broad scope gave way to the need to force attorneys to discuss reasonable approaches to discovery and clarify the guardrails, with thoughtful practitioners offering tools, models, and analysis designed to bring about the proportional approach to discovery outlined in the 2015 amendments.[47]

While U.S. lawyers grapple for a proportionality matrix, the data explosion continues to accelerate, and the burdens around it have changed to include data protection and privacy laws. Although this may seem like a large or asymmetrical litigation problem, the truth is compliance with data protection laws is now a discovery burden for both responding *and* requesting parties. Data types are more varied, volumes are higher, and data is hosted in more places than ever. Cross-border burdens associated with data protection and differences in culture, resources, and accessibility are a reality for more parties than ever before—not just corporate defendants responding to discovery requests. Social media, mobile phone applications, collaboration software, and the move to cloud computing has complicated this picture for everyone.[48]

Before issues of comity or conflicts of law even enter the analytical framework, it is important to remember that Rule 26(b)(1) is not limited to geography. It focuses on burdens and costs for both requesting and responding parties—regardless of where those come from or what law or regulation drives them.

---

[46] FED. R. CIV. P. 1.

[47] See Laporte & Redgrave, *supra* note 6, at 24; Hon. Paul W. Grimm, *Are We Insane? The Quest for Proportionality in the Discovery Rules of the Federal Rules of Civil Procedure*, 36 REV. OF LITIG. 117; *Discovery Proportional Model: A New Framework*, RABIEJ LITIGATION LAW CENTER, https://rabiejcenter.org/best-practices/ediscovery/ (last visited June 12, 2024); RONALD J. HEDGES, BARBARA JACOBS ROTHSTEIN & ELIZABETH C. WIGGINS, MANAGING DISCOVERY OF ELECTRONIC INFORMATION (3d ed. 2017).

[48] *See, e.g., Nichols v. Noom*, in which the discovery dispute was not simply about whether a particular group of documents were in scope, but whether the court should order a responding party to use "MetaSpike's Forensic Evidence Collector (""FEC"") to recollect Google Drive and Gmail documents so that any hyperlinked documents are also pulled as part of the document 'family' or to create a program using Google's application programming interface to extract links from responsive Google Drive documents, retrieve those linked documents, and produce them as attachments." Nichols v. Noom Inc., No. 20-CV-3677 (LGS) (KHP), 2021 WL 948646, at *1 (S.D.N.Y. Mar. 11, 2021). This, despite the court noting that in "this Court's experience, only a fraction of the documents produced in discovery will be material to the litigation." *Id.*

The above challenges notwithstanding, this *Commentary* recognizes that requesting parties are entitled to and do require relevant, nonprivileged documents to prosecute or defend their cases. The challenge is to implement a discovery scope proportional to the case's needs. Further complicating this challenge is that unlike most jurisdictions, the U.S. civil justice system has placed enforcement of many laws in the hands of litigants, acting as a quasi-private attorney general to seek redress and damages. Most other countries enforce many of their civil laws in the context of a state regulatory system.

This *Commentary* now addresses the added challenges posed by non-U.S. data protection laws.

III. NON-U.S. DATA PROTECTION LAWS

A. Introduction

Data privacy and protection laws have been around for years, and concerns about data privacy and protection go back more than a century. In 1890, for example, Samuel D. Warren and Louis D. Brandeis published an article in the Harvard Law Review entitled *"The Right to Privacy*."[49] They noted that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[50] They could have not imagined at the time the devices available today that "threaten" the privacy of the individual, and the ongoing challenge for governments faced with the question of how to protect individual privacy while balancing other rights.

Modern times have brought forward the development of various and varying laws outside the U.S. impacting privacy and the transfer of personal data.

Omnibus laws are comprehensive national data protection laws that apply to any person and organization within the nation's defined territorial scope. In some cases, individual regions within a country may have separate data protection laws, but without national cohesion.

Sectoral laws are data protection laws directed at specific industries or targeted groups of individuals. For example, bank secrecy laws can prevent the disclosure of confidential client data to third parties. Telecommunications laws may restrict the international transfer of personal data a telecommunication firm holds.

Blocking statutes, which are laws of a jurisdiction meant to hinder the application of foreign law, can make the implementation of data transfer requests even more difficult.[51]

---

[49] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[50] *Id.* at 195.

[51] Other confidentiality laws, such as blocking laws, state secret laws, and banking secrecy laws are enacted with the specific intent of depriving a foreign jurisdiction of access to data, rather than with the foremost intent of protecting the data and privacy of its citizenry. As such, U.S. judges are likely to accord less weight to those laws in their analysis of balancing the interest of the foreign state against the interest of the U.S. and the party seeking the information. *See*, *e.g.*, the French blocking statute whose Article 1 prohibits the provision of documents or information to foreign public authorities as harmful to the sovereignty, security, and economic interests of France and was drafted specifically as a regulator on U.S. discovery and attempt to require compliance with the Hague Evidence Convention. Loi 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères [Law 68-678 of July 26, 1968 relating to the communication of economic, commercial, industrial, financial or technical documents and information to foreign natural or legal persons], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], July 27, 1968, p. 7267, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000501326. The Decree No. 2022-207 of Feb. 18, 2022, which as of Apr. 1, 2022 requires any French legal or natural persons to report to French authorities a request from a foreign public authority falling

Any party tasked with transferring or processing data internationally for any reason, including in the context of litigation, must understand the privacy requirements, data protection requirements, and data transfer restrictions of all countries involved and the potential burdens these requirements might place on a party trying to comply with discovery requests or court orders from the U.S.

B. The European Union General Data Protection Regulation

Although data protection laws can vary in scope and focus, the exemplary legislation to be considered here is the European Union (EU) General Data Protection Regulation ("GDPR").[52] The GDPR was adopted in 2016 and became fully applicable on May 25, 2018.[53] The GDPR has been incorporated into the European Economic Area (EEA) Agreement, applying to all member states of the EEA, including the member states of the EU, Iceland, Lichtenstein, and Norway.[54] The GDPR has been incorporated as a base legislation but leaves room for derogations.[55]

The territorial scope of the GDPR is broad and intended to "ensure comprehensive protection of the rights of data subjects in the EU and to establish . . . a level playing field for companies active on the EU markets, in a context of worldwide data flows."[56] The law applies to "the processing of personal data in the context of the activities of an establishment of a controller or processor in [the EU], regardless of whether the processing takes place in the Union or not."[57] Thus, the extraterritorial reach of the GDPR extends to the processing of personal data of data subjects who are in the EU even when the controller or processor is not established in the EU, if the processing activities

---

under Article 1 of the 1968 blocking statute, is likely to only continue the trend of U.S. judges comparatively weighing in favor of U.S. interests and renew interests in the debate around whether compliance with the Hague Evidence Convention is mandatory or permissive. Décret 2022-207 du 18 février 2022 relatif à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères [The Decree 2022-207 of Feb. 18, 2022 relating to the communication of economic, commercial, industrial, financial or technical documents and information to foreign natural or legal persons], https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045190519.

52 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents [hereinafter GDPR].

53 *Id.*

54 *See General Data Protection Regulation incorporated into the EEA Agreement*, EUROPEAN FREE TRADE ASSOCIATION (July 6, 2018), https://www.efta.int/media-resources/news/general-data-protection-regulation-incorporated-eea-agreement.

55 *See id.*; GDPR, *supra* note 52.

56 European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1, 4 (Nov. 12, 2019), *available at* https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

57 GDPR, *supra* note 52, art. 3.1.

relate to any offering of goods or services to data subjects located in the EU (not just EU citizens)[58] or to the monitoring of the behavior of these data subjects while in the EU.[59]

Once an organization falls under the scope of the GDPR, multiple obligations are imposed on controllers and processors, which trigger additional tasks. For instance, the responsible data controller/processor must keep a record of the processing activities performed on the data.[60] The responsible party must also designate a Data Protection Officer if the processing falls under one of the cases laid down in the Regulation.[61]

A "controller" is the natural or legal person determining the purpose and means of the processing.[62] "Processing" is defined to include any operation performed on personal data, including its transfer.[63] "Personal data" means all data relating to an identified or identifiable person.[64] The understanding of "personal data" according to the GDPR is much broader than that of U.S. law.

Even when all of obligations required of a data processer/controller by the GDPR are met, data processing, which includes the preservation, collection, and analysis of personal data, will be lawful only if and to the extent that at least one of the following criteria involving the data subject is met:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

2. processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract;

3. processing is necessary for compliance with a legal obligation to which the controller is subject;[65]

4. processing is necessary to protect the vital interests of the data subject or of another natural person;

---

58 *Id.* art. 3.2(a).

59 *Id.* art. 3.2(b).

60 *Id.* art. 30.

61 *Id.* art. 37.

62 *Id.* art. 4(7).

63 *Id.* art. 4(2).

64 *Id.* art. 4(1).

65 As interpreted by the European Data Protection Board and EU Data Protection Authorities, Article 6(1)(c) is limited to legal obligations imposed by EU or member state national law. *See Compliance with a legal obligation of the controller*, EUROPEAN DATA PROTECTION BOARD, https://edpb.europa.eu/sme-data-protection-guide/process-personal-data-lawfully_en#toc-4 (last visited June 11, 2024).

5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[66]

Thus, the processing of personal data is lawful if the data is processed based on the consent of the data subject concerned or on another legitimate basis laid down by law.

The GDPR outlines explicitly that consent must be given by a clear affirmative act, establishing a freely given, specific, informed, and unambiguous indication of the individual's agreement to the processing of his/her data.[67] In practical terms though, many organizations may find relying on consent too great a challenge, given the problems that accompany effective consent, such as the proof of burden applying to the controller to establish that the GDPR requirements for lawful consent are met, or the consequences of the revocation of consent should the data subject invoke the right to withdraw consent at any time.

A party might seek to justify a data transfer and data processing in a litigation because it is "necessary for the purposes of the legitimate interests pursued by the controller," but the application of such a lawful basis requires balancing the interests of the controller and the individual data subject.[68] There are several factors that must be met in satisfying the legitimate interest condition: the processing must be necessary for the purpose; the purpose must be a legitimate interest for the controller or a third party; and the legitimate interest is not overridden by the data subject's interest or fundamental rights and freedoms.[69] Data controllers relying on legitimate interest should document the considerations of the balancing test in a Legitimate Interest Assessment, which records the controller's reasons for reliance on that ground and shows a proper decision-making process.[70] At the same time, in relying on the legitimate interest criterion, controllers must carefully consider its interpretation by local data protection regulators and courts, since it has historically been understood differently across the EU.

It is also essential that the "data minimization principle" is followed by limiting processing of personal data to what is relevant and strictly necessary and by erasing unnecessary material without

---

66 GDPR, *supra* note 52, art. 6.

67 *Id.* art. 7.

68 *Id.* art. 6(1)(f).

69 *See* GDPR Recital 47, https://www.privacy-regulation.eu/en/r47.htm.

70 *See, e.g.*, *Data Protection Toolkit - Legitimate Interests Assessment & Template*, NORTHERN IRELAND COUNCIL FOR VOLUNTARY ACTION (NICVA), https://www.nicva.org/data-protection-toolkit/templates/legitimate-interests-assessment-template (last visited June 11, 2024).

preserving it.[71] In the context of eDiscovery, this means taking steps to collect, process, and review only ESI that is necessary to the case. Parties would have to negotiate the appropriate discovery limitations to minimize the processing and transfer of unnecessary data, rather than allowing a fishing expedition for tangential information or data.

Finally, EU member states can maintain or introduce national provisions further specifying the application of the GDPR; for example, an EU member state may "have several sector-specific laws in areas that need more specific provisions."[72] Thus, a party charged with the international transfer of data falling within the territorial scope of a certain EU country would have to ensure that the data transfer conforms not only with the GDPR, but also with any other country-specific requirements.

1. Enforcement and Penalties

The enforcement of data privacy and data protection laws can vary by country and regulation, so the impact on a party that processes personal data can vary greatly depending on where the party and the data are based. Fines in the EU, for example, can be significant. Failure to comply with the GDPR with more minor infractions can result in fines as much as the amount equal to 2 percent of an organization's global annual turnover or EUR 10 million, whichever is higher.[73] For more serious infringements, including violating the basic principles for processing, the data subjects' rights, and rules regarding "the transfers of personal data to a recipient in a third country or an international organization," the penalty can be as much as 4 percent of the global annual turnover for an organization or EUR 20 million, whichever is higher.[74] Along with administrative fines, supervisory authorities in each EU member state are empowered to impose limitations, including a ban on processing, or to order the suspension of data transfers to a recipient in a third country.

2. The GDPR and Cross-Border Transfers of Personal Data

The entirety of Chapter V of the GDPR is devoted to the "transfers of personal data to third countries or international organizations."[75] Its goal is to ensure that the level of protection guaranteed by the GDPR is maintained during international transfers of personal data.[76] The provisions also "aim

---

71 GDPR, *supra* note 52, art. 5(1)(c).

72 GDPR Recital 10, https://www.privacy-regulation.eu/en/recital-10-GDPR.htm. For example, Article 88 of the GDPR specifically permits member states to provide "more specific rules" for the process of employees' personal data in the employment context.

73 GDPR, *supra* note 52, art. 83(4).

74 *Id.* art. 83(5).

75 *See id.* arts. 44–50.

76 *See id.* art. 44.

at ensuring the continued protection of personal data after they have been transferred."[77] International transfers of personal data may take place when certain requirements are met. First, international transfers of personal data are permissible when the European Commission has decided that the third country, territory, or organization has ensured an adequate level of protection that must be essentially equivalent to that guaranteed within the EU by the GDPR.[78] Without this adequacy decision from the European Commission, data may be transferred "only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available."[79]

Absent either an adequacy decision or the existence of appropriate safeguards, there are only a certain set of derogations that apply under specific conditions, by which the international transfer is lawful per the GDPR, including, for example, with the consent of the data subject, when it is necessary for the performance of a contract, for reasons of public interest, or for the "establishment, exercise or defense of legal claims."[80]

In July 2020, the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield ("Privacy Shield"), an international agreement between the EU and the U.S. outlining the level of protection necessary for exporting personal data from the EU to the U.S.[81] The CJEU ruled that transfers of data outside the EU/EEA are prohibited absent an adequacy decision by the European Commission and adequate safeguards, which the Privacy Shield failed to provide, and set the bar even higher with additional obligations for the data exporter to ensure the adequate protection of data before its export,[82] through the adoption of supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence.[83]

While these supplementary measures are still obligations, the European Commission's July 2023 adoption of the EU-U.S. Data Privacy Framework ("DPF") provides additional obligations for U.S. self-certifying organizations. Designed to directly address the CJEU's 2020 decision and improve

---

77 European Data Protection Board, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en.

78 GDPR, *supra* note 52, art. 45(1).

79 *Id.* art. 46(1).

80 *Id.* art. 49.

81 Data Prot. Comm'r v Facebook Ir. Ltd., Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559 (E.C.J. July 16, 2020), https://curia.europa.eu/juris/document/document.jsf;jsessionid=397BF5F2-AE797A24B87EAAC9B44BD809?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2596699.

82 *Id.*

83 *See* European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (June 18, 2021), *available at* https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

upon the Privacy Shield, the DPF requires personal information being transferred from the EU to the U.S. be limited to what is necessary and proportionate. It also improves upon data subject redress by allowing European data subjects to lodge inquiries and complaints about the transfer and use of their personal information that are subject to review by a Data Protection Review Court, which is empowered to independently investigate and resolve complaints through binding remedial measures.[84]

The international transfer of personal data protected by the GDPR can be avoided altogether if that private information is considered irrelevant to a matter in U.S. legal proceedings, because the personal data could be excluded from the transfer via redaction or anonymization.[85] Should personal information be required in a U.S. legal context, however, there are limited legal exceptions within the GDPR. The GDPR specifies that decisions from third-country authorities, courts, or tribunals are not in and of themselves legitimate grounds for data transfers to a non-EEA country, unless based on an international agreement such as a mutual legal assistance treaty.[86]

One possible basis for the legal transfer of data would be when the "processing is necessary for the purposes of the legitimate interests pursued by the controller."[87] Yet applying this exception requires strictly balancing the interest of the controller and the individual as noted above.[88]

The processing of personal data by "competent authorities" such as a court is another possible exemption.[89] But this is limited to the information being transferred directly to the court "for the purposes of the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties."[90] Although compliance with a legal obligation to which a controller is subjected can justify the processing of data in some circumstances,[91] according to the European

---

84 European Commission Press Release, Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows (July 10, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721; *see also* full text of the European Commission adequacy decision for the EU-US Data Privacy Framework, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, *available at* https://commission.europa.eu/document/download/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en?filename=Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf..

85 GDPR Recital 26, https://www.privacy-regulation.eu/en/recital-26-GDPR.htm.

86 GDPR, *supra* note 52, art. 48.

87 *Id.* art. 6(1)(f).

88 *Id.* The factors involved in satisfying the legitimate interest condition include that the processing must be necessary for the purpose; the purpose must be a legitimate interest for the controller or a third party; and the legitimate interest cannot be overridden by the data subject's interest or fundamental rights and freedom. *See* GDPR Recital 47, https://www.privacy-regulation.eu/en/r47.htm.

89 GDPR, *supra* note 52, art. 2.2(d).

90 *Id.*

91 *Id.* art. 6(1)(c).

Data Protection Board, an order from a U.S. court alone does not serve as an applicable legal ground for the transfer of personal data to the U.S.[92]

One possible litigation exception as outlined in GDPR Article 49(1)(e) allows transfers to take place as a "Derogation for specific situations" when "the transfer is necessary for the establishment, exercise or defense of legal claims."[93] This can cover a wide range of activities, including "transfers for the purpose of formal pre-trial discovery procedures in civil litigation."[94] But the wording of the derogation applies only to "a transfer or set of transfers of personal data," and not to any processing that might be required. As a derogation it is also not designed to apply to repetitive transfers.[95] A particular consideration for applying this possible litigation exception is the limitation that the transfer be "**necessary** for the establishment, exercise or defense of the legal claim in question."[96] This "necessity test" requires a "close and substantial connection between the data in question" and the particular legal claim[97] and must be "compelling" when balanced against the "rights and freedoms of the data subject."[98]Thus a party required to disclose personal data to a U.S. court would have to carefully substantiate the relevance to the particular matter, creating another hurdle for the party involved before the legal transfer of data and creating more potential risk for the party should it misjudge the need for the data to the case.

If an organization follows a U.S. court order and transfers data to the U.S. without adequate privacy protection and safeguards, the European data protection authorities could seek to impose the fines as noted above. Yet refusing to transfer the requested data because of concerns about following data protection law may lead a U.S. court to impose sanctions, including contempt. Thus, parties involved in legal matters requiring the transfer to the U.S. of personal data falling under international data privacy and protection laws may be stuck between a rock and a hard place regarding the obligation to fulfill requests for data in the U.S. and the obligations to protect that data and individual privacy under the applicable laws of the other territories involved.

C. Non-EU Jurisdictions

Although this *Commentary* follows the lead of prior Sedona Conference commentaries in using the EU's GDPR as a model for identifying and addressing cross-border discovery challenges associated

---

92 European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (May 25, 2018) 5, *available at* https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

93 GDPR, *supra* note 52, art. 49(1)(e).

94 EDPB Guidelines 2/2018 on derogations of Article 49, *supra* note 92, at 11.

95 GDPR, *supra* note 52, art. 49.

96 EDPB Guidelines 2/2018 on derogations of Article 49, *supra* note 92, at 12 (emphasis in original).

97 *Id.*

98 GDPR, *supra* note 52, art. 49.

with foreign data protection and privacy compliance, many countries in the world now have some sort of data protection law addressing privacy rights.[99] Some of these "comprehensive data privacy laws" were modeled after the GDPR, but not all. China, for example, continues building on data protection laws that are tied not only to the rights of its citizens, but also to national security concerns. Given the proliferation of global data protection regulation, it is worth at least noting those laws here in the context of their impact on U.S. discovery scope assessments and proportionality. They all have provisions detailing individual rights (access, correct, delete), business obligations (notice/transparency, legal basis for processing, purpose limitations, data minimization, record keeping, breach notification, data protection officers) and enforcement (fines, criminal penalties, personal liability, private right of action).[100]

The requirements to comply with these provisions and avoid civil or criminal liability similarly impacts burdens and costs connected to identifying, preserving, collecting, reviewing, and producing relevant discovery. Practical challenges connected with compliance may also affect the analysis associated with the remaining five proportionality factors.

1. United Kingdom (UK)

The UK enacted its own data protection law following its departure from the EU. The primary provisions, however, closely track the GDPR in terms of: processing definitions and principles, territorial scope, defining personal information, lawful basis, transparency, data minimization, transfers, necessity, and proportionality.[101] In addition, as of October 12, 2023, organizations in the UK who are certified under the "UK Extension to the EU-US DPF" can transfer personal data to the U.S. under Article 45 of the UK GDPR.[102]

As a practical matter, this means that U.S. discovery sought in the UK will have to undergo a similar analysis to ensure compliance.

---

[99] *Global Comprehensive Privacy Law Mapping Chart*, IAPP (Apr. 2022), https://iapp.org/media/pdf/resource_center/global_comprehensive_privacy_law_mapping.pdf.

[100] *Id.*

[101] *Commentary on Managing International Legal Holds, supra* note 10, at 188–89 (citing to https://uk-gdpr.org/wp-content/uploads/2022/01/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.).

[102] *Notice: UK-US data bridge: factsheet for UK organisations*, DEPT. FOR SCI., INNOVATION & TECH. (Sept. 21, 2023), https://www.gov.uk/government/publications/uk-us-data-bridge-supporting-documents/uk-us-data-bridge-fact-sheet-for-uk-organisations.

2. Asia-Pacific (APAC)

a. Australia

Australia, like the U.S., has a mix of federal, state, and territorial data protection laws. However, the federal Privacy Act contains the Australian Privacy Principles applying to private organizations with at least AUD $3 million. Collection and processing of personal information under the Privacy Act must be purpose limited based on disclosure, consent, or required by law. Disclosure associated with transfer to an organization outside of Australia can be based on a legal requirement or authorization, including as ordered by a court.[103]

b. China

China has multiple data protection laws impacting cross-border discovery, but the three primary ones are the Personal Information Protection Law (PIPL), the Cybersecurity Law (CSL), and the Data Security Law (DSL). The CSL and DSL pre-date the PIPL and focus respectively on regulating cybersecurity impacting critical, network, and personal information and general data security across a broad range of data. The PIPL represents China's "comprehensive" data protection law regarding individual privacy.

PIPL notably requires express and informed consent from data subjects for processing personal information and explicit consent tied to the specific processing activity if the activity involves: sensitive personal information, overseas transfers, public disclosure of personal information, or provision of data to another data controller for processing. Like the GDPR, there are also lawful bases for processing that include fulfilling legal obligations. Yet unlike the GDPR, lawful basis has not appeared to be heavily relied on in cross-border discovery, and there is still uncertainty around the extent it can be relied on.[104]

One example of this uncertainty in a U.S. discovery context can be seen in *Cadence Design Systems v. Syntronic AB*, a recent case from the Northern District of California involving a motion to compel discovery from China. Although the magistrate ultimately ruled for compelling production of discovery from computers, the decision centered on a close analysis and debate among party experts around both the translation of and ultimate requirements regarding consent.[105]

The Cyberspace Administration of China (CAC) acts as the primary regulator on the PIPL and ensures that cross-border transfers comply with lawful basis requirements (security assessments, CAC certification, standard contractual clauses (SCCs)), implements necessary protective measures (due

---

[103] *Data Protection Laws of the World: Australia,* DLA PIPER (Dec. 31, 2023), https://www.dlapiperdataprotection.com/index.html?c=AU&t=definitions#.

[104] *Data Protection Laws of the World: China,* DLA PIPER (Apr. 29, 2024), https://www.dlapiperdataprotection.com/index.html?t=law&c=CN.

[105] Cadence Design Sys. v. Syntronic AB, No. 21-cv-03610-SI (JCS), 2022 WL 2290593 (N.D. Cal. June 24, 2022).

diligence, contractual protections and monitoring), ascertains the above-mentioned explicit consent, and conducts a privacy impact assessment. Enforcement and penalties for noncompliance with PIPL include: notices and warnings; administrative fines up to 5 percent of the previous year's annual revenue; cessation of processing; suspension of applications or services; suspension of business; suspension of management/official's role; criminal sanctions; civil claims; and negative impacts to social or business credit scoring.[106]

c. Japan

Japan's amended Act on the Protection of Personal Information (APPI) went into effect in 2022 and focuses primarily on regulating the use of personal information by business operators. The Personal Information Protection Commission (PPC) regulates privacy issues through interpretation and enforcement of the APPI.

Business operators are required to provide notice to data subjects describing the purpose of use of their personal information and are not allowed to use personal information beyond the defined scope. Transfer of personal information to third parties requires consent, and transfers outside of Japan require consent specifically informing the data subject of the receiving country. There are also requirements ensuring transfer to a country with adequate standards of data protection. A 2019 Japanese adequacy decision found the UK and EU adequate, and international frameworks such as the APEC Cross-Border Privacy Rules System are recognized as providing "similarly adequate standards." Organizations are advised to assign privacy officers, despite there being no legal requirement for a data protection officer. Enforcement and penalties through the PPC may include: reporting requirements with associated fines up to JPY 500,000; on-site inspections; remedial actions; imprisonment of organization officers, representatives, or managers for up to one year or fines of JPY 1,000,000 for noncompliance with a PPC order; and unauthorized disclosure of personal information penalties of up to one year or a fine of up to JPY 500,000 or JPY 1 million if the disclosing party is a legal entity.[107]

Cross-border discovery might be further complicated by the fact that Japan does not have comparable civil procedure requirements around broad discovery and disclosure. While requesting parties may ask the court to order discovery, the request must be specific as to the documents, describe what the documents contain and include a legal basis. In practice, obtaining discovery can be difficult.[108]

As a result of the above data protection requirements and local approach to discovery, parties in U.S. litigation seeking discovery from Japan face an element of uncertainty around collecting,

---

[106] *Data Protection Laws of the World: China*, *supra* note 104.

[107] *Data Protection Laws of the World: Japan,* DLA PIPER (Jan. 1, 2024), https://www.dlapiperdataprotection.com/index.html?t=law&c=JP.

[108] *Global Attorney-Client Privilege Guide: Japan*, BAKER MCKENZIE, https://resourcehub.bakermckenzie.com/en/resources/global-attorney-client-privilege-guide/asia-pacific/japan/topics/01—-discovery (last visited June 11, 2024).

processing, and transferring data to requesting parties. While the GDPR is robust and can be challenging to interpret, its approach to data privacy as a fundamental right makes it clear that regulation is not meant to be limited to commercial utilization of personal information. Similarly, both EU and EU member states have narrow disclosure scope obligations compared to the U.S., but somewhat broader than Japan. The EU has, however, recognized Japan as having adequate protections through a European Commission adequacy decision. This suggests that GDPR-like safeguards may be required for cross-border discovery. Responding parties, however, will have to decide whether consent is required for cross-border discovery to a country that is not whitelisted by Japan for a lawful basis that has no root in Japanese procedural law.

3. Latin America

a. Argentina

The European Commission has also deemed Argentina's Personal Data Protection Law (Law 25.326) adequate. Collection and processing of personal information must be informed, purpose limited, and based on consent unless there is a lawful basis, which can include legal obligations. Enforcement is handled by the Agency for Access to Public Information (*Agencia de Acceso a la Informacion Publica*).

Personal data transfers generally may occur only for legitimate purposes and usually with the prior consent of the data subject, which can be revoked. Cross-border data transfers to countries without adequate protections are prohibited absent express consent, unless necessary for international judicial cooperation or in the context of international treaties. Enforcement and penalties include potential fines, criminal charges including prison, and civil actions to access, correct, suppress, update, or protect personal information through proper confidentiality designations.[109]

b. Brazil

Personal information in Brazil is regulated by the Brazilian General Data Protection Law ("LGPD") as administered by the National Data Protection Authority ("ANPD"). The ANPD has authority to issue sanctions for violating the LGPD. The collection and processing of personal data are referred to as "data treatments," requiring a lawful basis including, but not limited to: consent, compliance with a legal obligation of the controller, exercising legal rights, and to fulfill the legitimate interests of a controller or third party as balanced against the fundamental rights and freedoms of the data subject.

Cross-border transfers of personal information require prior specific and informed consent, unless the transfer: is to another country with adequate levels of protection, is completed with adequate

[109] *Data Protection Laws of the World: Argentina,* DLA PIPER (Jan. 28, 2024), https://www.dlapiperdataprotection.com/index.html?t=law&c=AR.

guarantees of protection (SCCs, specific clauses for a particular transfer), or is necessary for compliance with a legal or regulatory obligation or exercise of rights in a judicial procedure.

Enforcement and penalties for violating the LGPD include: administrative sanctions; incremental fines up to 2 percent of the revenue of a private legal entity up to a maximum of R$50 million per infraction; warnings; publication of the violation; blocking personal data access until remediation; deletion of personal data; suspension of database operation for a period up to six months; suspension of personal data processing activity related to the violation for a period up to six months; and partial or total prohibition of activities related to data processing.[110]

[110] *Data Protection Laws of the World: Brazil,* DLA PIPER (Jan. 28, 2024), https://www.dlapiperdataprotection.com/index.html?t=enforcement&c=BR&c2=.

IV. COMITY CONSIDERATIONS

U.S. courts have invoked the doctrine of "comity" to reconcile conflicts between non-U.S. laws and U.S. discovery practices. Comity refers to the "spirit of cooperation" required of U.S. courts to resolve issues affecting other sovereign states' laws and interests.[111] The U.S. Supreme Court has recognized the need for "due respect" for foreign laws and set out certain factors to consider in any comity analysis.

A. Hague Convention

The United States and 65 other nations have entered into the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (Hague Convention) as contracting member states.[112] The Convention "prescribes certain procedures by which a judicial authority in one contracting state may request evidence located in another"[113] and came into force on October 7, 1972. It was the direct outgrowth of the 1964 Tenth Session discussions around improving the provisions of the 1954 Civil Procedure Convention dealing with taking of evidence abroad and driven in part by suggestions from the United States that alternatives to letters rogatory be considered.[114]

The Hague Convention is an international treaty and comprises two separate and independent systems for the taking of evidence abroad. Chapter I outlines the taking of evidence through letters rogatory or "Letters of Request" issued by legal authorities in one contracting jurisdiction to another. Chapter II outlines the taking of evidence through Consuls and Commissioners. Both systems can be utilized, are self-contained, and are not mutually exclusive. This means that although there are considerations as to which system would make the most sense in any given scenario, either could be chosen, and the selection does not prevent the concurrent utilization of the other. They are self-contained in that the steps involved for each are unique to each and cannot not be used to satisfy the requirements of the other.[115]

A central question to the operation of the Hague Convention has been whether it is mandatory. Generally, civil law countries such as France and Germany have historically viewed the Hague Convention as mandatory, requiring compliance with either Chapter I or II if a contracting jurisdiction is seeking evidence from another. Common law countries such as the United States have historically viewed the Hague Convention as nonmandatory, meaning parties seeking evidence from a

---

[111] Gucci Am., Inc. v. Weixing Li, 768 F.3d 122, 126 (2d Cir. 2014).

[112] Hague Conference on Priv. Int'l Law [HCCH], Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters: Number of Contracting Parties to this Convention, https://www.hcch.net/en/instruments/conventions/status-table/?cid=82 (last visited June 11, 2024).

[113] Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for the S. Dist. of Iowa, 482 U.S. 522, 524 (1987).

[114] HAGUE CONFERENCE ON PRIV. INT'L LAW, PRACTICAL HANDBOOK ON THE OPERATION OF THE EVIDENCE CONVENTION, at 3 (4th ed. 2020).

[115] *Id.* at 8.

contracting jurisdiction may, but are not obligated to, use the Hague Convention. In addition, some countries, such as Italy and Spain, exclude Article 23 (pretrial discovery of documents) from Chapter II but adhere to other provisions such as the utilization of diplomatic officers or consular agents. In the context of a United States court order compelling discovery, for example, still other countries, such as Portugal, do not adhere to Chapter II, Article 18 (assistance to obtain evidence by compulsion).[116]

In *Aérospatiale,* the U.S. Supreme Court held that the Hague Convention does not provide the exclusive means for obtaining evidence abroad.[117] Rather, the Court recognized that in certain instances, such as when a court lacks personal jurisdiction, the Hague Convention may yield "evidence abroad more promptly than use of the normal procedures governing pre-trial civil discovery," and such instances will lead to "first-use strategy."[118] The Court set out factors for district courts to consider on a case-by-case basis when determining whether a party should have to seek discovery through the Hague Convention, or whether a party may proceed under the Federal Rules of Civil Procedure.

B. Comity Analysis

In the wake of *Aérospatiale*, district courts are responsible for analyzing the facts for each case and assessing the likelihood that Hague Convention procedures would be effective. "[D]etermining whether to require a party to follow the Hague Convention protocol to obtain discovery requires 'scrutiny in each case of the particular facts, sovereign interests, and likelihood that resort to those procedures will prove effective.'"[119]

Courts have applied a two-step approach to determine whether the requested discovery at issue must be pursued through Hague Convention procedures. First, the party seeking protection from discovery (or application of the Hague Convention procedures) must show that production of the discovery sought conflicts with a foreign law.[120]

Second, the court must apply a comity analysis to balance the interest of the foreign state against the interest of the U.S. and the party in obtaining the information.[121]

---

116 *Id.* at 10–16.

117 *Aérospatiale*, 482 U.S. at 547.

118 *Id.* at 542 n.26.

119 Sun Grp. U.S.A. Harmony City, Inc. v. CRRC Corp., No. 17-CV-02191-SK, 2019 WL 6134958, at *1 (N.D. Cal. Nov. 19, 2019) (quoting *Aérospatiale*, 482 U.S. at 544).

120 EFG Bank AG v. AXA Equitable Life Ins. Co., No. 17-CV-4767 (JMF), 2018 WL 1918627, at *1 (S.D.N.Y. Apr. 20, 2018) (party seeking an order to apply Hague Evidence Convention procedures must identify a specific foreign law that "actually bars the production" at issue); *Sun Group U.S.A.*, 2019 WL 6134958, at *4 (same).

121 Grupo Petrotemex, S.A. De C.V. v. Polymetrix AG, No. 16-cv-2401 (SRN/HB), 2019 WL 2241862, at *2 (D. Minn. May 24, 2019) ("[A] party seeking to require that discovery be obtained through Hague Convention international discovery procedures must 'demonstrate appropriate reasons for employing [them].'") (quoting *Aérospatiale*,

Under the second step of this analysis, the U.S. Supreme Court set out the following factors to any comity analysis: "(1) the importance to the . . . 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 important interests of the state where the information is located."[122] The Court noted that these factors are not exhaustive.[123]

U.S. courts have also considered three additional factors: the hardship of compliance on the party or witness from whom discovery is sought; the likelihood of compliance; and whether the parties have entered a protective order to protect the disclosure of personal information.[124]

This section discusses each of these elements in turn:

1. **Importance of the Documents and ESI.** "Where the outcome of litigation 'does not stand or fall on the present discovery order,' or where the evidence sought is cumulative of existing evidence, courts have generally been unwilling to override foreign [privacy] laws."[125] Notably, "importance" of the information is a factor under both comity and Rule 26(b)(1) analyses.

2. **Specificity of the Requests.** "[G]eneralized searches for information, disclosure of which is

482 U.S. at 547) (alterations in original); Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1474 (9th Cir. 1992) ("The PRC's admitted interest in secrecy must be balanced against the interests of the United States and the plaintiffs in obtaining the information."); Randall v. Offplan Millionaire AG, No. 6:17-cv- 2103-Orl-31TBS, 2019 WL 1003167, at *6 (M.D. Fla. Mar. 1, 2019) (applying *Aérospatiale* comity analysis to determine whether to compel use of Hague Convention procedures).

122 *Aérospatiale*, 482 U.S. at 544 n.28 (citations and quotations omitted).

123 *See also International Litigation Principles*, *supra* note 2, at 9–10, which also discusses comity under *Aérospatiale*.

124 *Richmark*, 959 F.2d at 1475 (9th Cir. 1992) (considering "the extent and the nature of the hardship that inconsistent enforcement would impose upon the person" and "the extent to which enforcement by action of either state can reasonably be expected to achieve compliance with the rule prescribed by that state") (citation and quotations omitted); Inventus Power v. Shenzhen Ace Battery, No. 20 CV 3375, 2021 WL 4477940, at *13 (N.D. Ill. Sept. 30, 2021); Wultz v. Bank of China Ltd., 910 F. Supp. 2d 548, 553 (S.D.N.Y. 2012); AnywhereCommerce, Inc. v. Ingenico, Inc., No. 19-CV-11457-IT, 2021 WL 2256273, at *3 (D. Mass. June 3, 2021). At least one other court has also considered whether the person resisting discovery is a party to the litigation and, "[w]here the issue is the application of another country's privacy laws, . . . whether such privacy requirements are absolute." Tansey v. Cochlear Ltd., No. 13–CV–4628 SJF SIL, 2014 WL 4676588, at *2 (E.D.N.Y. Sept. 18, 2014) (citation omitted).

125 *Richmark*, 959 F.2d at 1475 (quoting *In re* Westinghouse Elec. Corp. Uranium Contracts Litig., 563 F.2d 992, 999 (10th Cir. 1977); Salt River Project Agric. Improvement & Power Dist. v. Trench France SAS, 303 F. Supp. 3d 1004, 1008 (D. Ariz. 2018) ("'Where the evidence is directly relevant' . . . . this factor weighs against utilizing Hague procedures.") (quotations omitted).

prohibited under foreign law, are discouraged."[126]

3. **Location of the evidence.** "[T]he Court looks to whether 'the documents to be disclosed and people who will produce those documents are located in a foreign country' or in the United States. If the determination is a foreign country, this factor weighs against compelling production."[127]

4. **Availability of alternative means.** "If the information sought can easily be obtained elsewhere, there is little or no reason to require a party to violate foreign law."[128]

5. **National interest.** Several courts, including the Ninth Circuit, have held that the interest of the foreign sovereign "is the most important factor" under this analysis.[129] In considering the interest of the foreign state, courts analyze "the significance of disclosure in the regulation . . . of the activity in question," and "indications of the foreign state's concern for confidentiality prior to the discovery."[130]

   Under this factor, courts typically examine whether a foreign data protection law will be violated by disclosure of the information sought.[131] For example, in *Knight Capital Partners Corp. v. Henkel Ag & Co.,* German defendants argued that "the German Federal Data Protection Act bars their production of all of the information that the plaintiff seeks, because all of the documents requested inherently would include 'personal information' of persons who are employed by or do business with Henkel, such as their names, email addresses, and calendar and phone records."[132] The court concluded that the interest of the United States in

---

[126] *In re* Mercedes-Benz Emissions Litig., No. 16-cv-881 (KM) (ESK), 2020 WL 487288, *7 (D.N.J. Jan. 30, 2020); *Salt River Project*, 303 F. Supp. 3d at 1008 (D. Ariz. 2018) ("Broad, generalized requests for information weigh in favor of utilizing Hague procedures, while specific, limited requests disfavor the use of Hague procedures.").

[127] *In re Mercedes-Benz,* 2020 WL 487288, at *7 (citations omitted); *Richmark*, 959 F.2d at 1475 ("The fact that all the information to be disclosed (and the people who will be deposed or who will produce the documents) are located in a foreign country weighs against disclosure, since those people and documents are subject to the law of that country in the ordinary course of business.").

[128] *Richmark*, 959 F.2d at 1475; Sun Grp. U.S.A. Harmony City, Inc. v. CRRC Corp., No. 17-CV-02191-SK, 2019 WL 6134958, at *4 (N.D. Cal. Nov. 19, 2019) (if parties cannot obtain documents necessary to litigate their claims through the Hague Convention, then "the balance would tip towards weighing in favor of full discovery through the Federal Rules of Civil Procedure."); *Salt River Project*, 303 F. Supp. 3d at 1009 ("[I]f the [Hague Convention] procedures are unsuccessful, the Court retains power to order discovery under the Rules.").

[129] *Richmark*, 959 F.2d at 1476; S.E.C. v. Gibraltar Glob. Sec., Inc., No. 13 CIV. 2575 GBD JCF, 2015 WL 1514746, at *5 (S.D.N.Y. Apr. 1, 2015).

[130] *Richmark*, 959 F.2d at 1476 (internal quotations omitted).

[131] *E.g.*, Finjan, Inc. v. Zscaler, Inc., No. 17-cv-06946-JST , 2019 WL 618554, at *3 (N.D. Cal. Feb. 14, 2019) ("considering the significant American interest in protecting its patents and the reduced U.K. interest in protecting the privacy of its citizens").

[132] Knight Cap. Partners Corp. v. Henkel Ag & Co., 290 F. Supp. 3d 681, 687 (E.D. Mich. 2017).

vindicating the rights of American plaintiffs was not outweighed by the "concerns of the German government with protecting its citizens from unjustified compromises of their personal information[.]"[133] The court further noted the German statute at issue "expressly allows disclosures that are necessary for the purposes of litigation[.]"[134]

6. **Hardship.** If the foreign national is "likely to face criminal prosecution" in its home country for complying with the U.S. court order, "that fact constitutes a 'weighty excuse' for nonproduction."[135]

7. **Likelihood of compliance.** "If a discovery order is likely to be unenforceable, and therefore to have no practical effect, that factor counsels against requiring compliance with the order."[136]

8. **Existence of a protective order:** A final consideration that courts look to is the existence of a protective order that would protect the disclosure of personal information made in response to discovery requests. Courts are more likely to grant discovery requests for data covered under foreign data protection laws where the parties have agreed to, and the court has entered, a robust protective order protecting information from further disclosure.[137]

Notably, the *Aérospatiale* Court held that non-U.S. laws prohibiting the production of documents in U.S. discovery is not dispositive.[138]

---

[133] *Id.* at 691 (citation omitted).

[134] *Id.* Although *Knight* predates both the 2018 GDPR and the implementation of the German Federal Data Protection Act (the Bundesdatenschutzgesetz or 'BDSG'), it is still representative of the typical approach of U.S. courts.

[135] *Richmark*, 959 F.2d at 1477 (quoting Société Internationale Pour Participations Industrielles Et Commerciales, S. A. v. Rogers, 357 U.S. 197, 211 (1958)).

[136] *Richmark*, 959 F.2d at 1478.

[137] AnywhereCommerce, Inc. v. Ingenico, Inc., No. 19-CV-11457-IT, 2021 WL 2256273, at *3 (D. Mass. June 3, 2021) (recognizing that disclosure under the court-ordered protective order was "[c]onsistent with the objectives of the GDPR"); *Knight,* 290 F. Supp. 3d at 691 (considering that the documents will be produced under a protective order governing their confidentiality.) Some courts have considered the existence of a protective order under the fifth category of the *Aérospatiale* analysis, which balances the interests of the United States with the interests of the foreign country. *See, e.g.*, *In re* Air Crash at Taipei, Taiwan on Oct. 31, 2000, 211 F.R.D. 374, 379 (C.D. Cal. 2002) (noting that the presence of a protective order lessened concerns about the foreign government's interest in maintaining secrecy over the disclosed materials); Finjan, Inc. v. Zscaler, Inc., No. 17CV06946JSTKAW, 2019 WL 618554, at *3 (N.D. Cal. Feb. 14, 2019) (noting the information sought would be marked confidential under the protective order); Fenerjian v. Nong Shim Co., No. 13CV04115WHODMR, 2016 WL 245263, at *5 (N.D. Cal. Jan. 21, 2016) (finding the protective order "adequately addresses the privacy concerns expressed in" the foreign data privacy law).

[138] Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for the S. Dist. of Iowa, 482 U.S. 522, 544 n.29 (1987) (observing that it is "well settled that [non-U.S. laws limiting discovery] do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute") (citing *Rogers*, 357 U.S. at 204–06).

V. U.S. PROPORTIONALITY RULES APPLIED IN CROSS-BORDER CONTEXT

U.S. federal courts address cross-border discovery issues under Rule 26 in various and inconsistent ways. Some courts have addressed cross-border issues in the Rule 26(b)(1) scope analysis, while others have addressed cross-border issues only in the context of the "comity" analysis under the U.S. Supreme Court's *Aérospatiale* framework. There are courts that conflate the proportionality and comity analyses and still others that first consider discoverability under Rule 26 and proceed to a comity analysis.

The variability in discovery scope analysis as applied to cross-border discovery fact patterns, particularly those involving compliance with foreign data privacy laws, is problematic and costly. Lack of predictability negatively impacts both requesting and responding parties and can be the oxygen feeding the flames of the type of discovery disputes the 2015 amendments were meant to avoid.

A. Consideration of Cross-Border Issues in Rule 26(b)(1) Scope Analysis

Several courts used Rule 26(b)(1) to hold that discovery of documents or information outside the U.S. is not permissible, based on relevancy, proportionality, or both. For example, in *In re Benicar (Olmesartan) Products. Liability Litigation*, a dispute arose over the plaintiffs' motion to compel defendants to produce their European affiliate's documents. The court denied the plaintiffs' motion, explaining that "just because defendants" have "control" over the ex-U.S. affiliate's documents does not necessarily mean defendants will be directed to answer plaintiffs' document requests."[139] And because "plaintiffs' document requests are overbroad and far-reaching," the court concluded, it would "not direct defendants to respond."[140] Yet the court made "clear" that its decision did not "foreclose an Order directing defendants to respond to appropriate document requests asking for relevant [European affiliate's] documents that [had] not already been produced."[141] The Court explained that "[i]nstead of general and overbroad requests, however, plaintiffs' requests must be specific, focused and narrow."[142]

Similarly, some courts have declined to permit discovery of ESI held by multinational or ex-U.S. entities where doing so would be cumulative of readily discoverable documents within the U.S. For example, in *In re Bard IVC Filters Products Liability Litigation*, patients filed products liability actions against a global medical device manufacturer. Plaintiffs sought "discovery of communications

---

[139] *In re* Benicar (Olmesartan) Prods. Liab. Litig., No. 15-2606 (RBK/JS), 2016 WL 5817262, at *7 (D.N.J. Oct. 4, 2016).

[140] *Id.*

[141] *Id.*

[142] *Id.* ("The Court will consider directing defendants to produce additional documents from Daiichi Europe but only if plaintiffs satisfy the Court the requests are well-grounded, materially relevant and non-cumulative."); *cf.* Corel Software, LLC v. Microsoft Corp., No. 2:15-cv-00528, 2018 WL 4855268, at *1 (D. Utah Oct. 5, 2018) (ordering retention and production of data relevant in a patent infringement case that Microsoft claimed "raises tension" with the GDPR and would require burdensome steps to anonymize).

between the [non-U.S.] entities and [non-U.S.] regulatory bodies regarding the [product] at issue in this case."[143] The court held that the non-U.S. subsidiaries' ESI regarding communications with foreign regulators was not relevant or discoverable, and the burden of accessing, identifying, and discovering such communications outweighed the benefit. In analyzing proportionality, the court concluded "that the burden and expense of searching ESI from 18 foreign entities over a 13-year period outweighs the benefit of the proposed discovery—a mere possibility of finding a [non-U.S.] communications inconsistent with United States communication."[144]

B. Consideration of Foreign Laws as Part of the Comity Analysis

Both before and after the 2015 amendments to Rule 26(b)(1), many courts have considered conflicts with foreign laws in the context of a comity analysis. A few courts have prohibited cross-border discovery based on finding that the requested discovery would violate foreign law, without undertaking the full-scale *Aérospatiale* analysis. For example, the district court in *Salerno v. Lecia, Inc.*[145] refused to compel production of certain documents sought since such discovery was prohibited by foreign law. In *Salerno*, the plaintiffs moved to compel discovery of European nationals' personnel and severance documents.[146] Citing foreign data protection laws, the court held that "the type of information sought by plaintiff is considered 'personal data' which cannot be disclosed to third parties located within the United States absent consent of the employee or assurances that the information will be subject to the same level of confidentiality protection."[147] Therefore, the court refused to compel production of data related to severance package and personnel files because it would expose the defendants to liability under the EU Directive and the German Data Production Act.[148]

Most courts, however, have considered the foreign law conflict only within the *Aérospatiale* comity framework. As discussed above, that framework involves a two-step approach of first establishing the foreign law conflict, then undertaking the weighing of *Aérospatiale's* enumerated factors. The party opposing discovery bears the burden of establishing that production would violate foreign law. Only after the party opposing discovery establishes that discovery will violate foreign law will the court proceed with a comity analysis.[149]

---

143 *In re* Bard IVC Filters Prod. Liab. Litig., 317 F.R.D. 562, 563 (D. Ariz. 2016).

144 *Id.* at 566.

145 Salerno v. Lecia, Inc., No. 97–CV–973S(H), 1999 WL 299306, at *3–4 (W.D.N.Y Mar. 23, 1999).

146 *Id.*, at *1.

147 *Id.* at *3.

148 *Id.*

149 Laydon v. Mizuho Bank, Ltd., 183 F. Supp. 3d 409, 413 (S.D.N.Y. 2016) ("Once a foreign law is found to conflict with domestic law, courts perform a comity analysis to determine the weight to be given to the foreign jurisdiction's law.") (internal quotations omitted).

While briefly acknowledging Rule 26 and the Federal Rules' "usual liberal approach to discovery," one court's analysis focused only on whether the "need for deference to a foreign sovereign entity" precluded discovery under the *Aérospatiale* factors. *In re Payment Card Interchange Fee & Merchant Discount Antitrust Litigation* involved a discovery dispute over two documents created in connection with the European Commission's investigations into the defendants' conduct.[150] "The Commission declined to authorize production . . . relying on 'the European Commission's general policy that the Statement of Objections and the information contained therein should be used only for the purpose of proceedings concerning the application of [European competition law].'"[151] The court, ruling on a motion to compel, applied *Aérospatiale* to conclude that the "Commission's interest in confidentiality outweighs the plaintiffs' interest in discovery of the European litigation documents."[152] The court reached this conclusion largely because the European Commission asserted that it desired to "restrict access to its own investigative and adjudicative procedures" and had "filed briefs in several district courts seeking to vindicate that interest."[153] Specifically, the court recognized the significance of the confidentiality of the investigative and adjudicative procedures for effective enforcement of European antitrust law because: (1) such "confidentiality encourages third parties to cooperate with the Commission's investigations," and (2) the Commission "relies on information provided by complainants and other third parties, including business secrets and other information that the third parties often want to keep confidential."[154] In addition, the plaintiffs already had access to "an unredacted copy of the extensive opinion published by the Commission."[155] Therefore, the court denied the plaintiffs' motion to compel.

Many courts have held that U.S. interests in full discovery outweigh the interests of foreign jurisdictions. For example, *Devon Robotics v. DeViedma* involved broad discovery requests related to claims for breach of fiduciary duty, tortious interference with contract, and defamation. The defendant moved for a protective order to prevent disclosure, arguing that his employer owned the documents and that their disclosure was prohibited by Italian privacy laws.[156] The court denied the motion, citing to *Aérospatiale* for the proposition that "[i]t is well settled that [a non-U.S. nondisclosure] statute [ ] do[es] not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute."[157] Applying the *Aérospatiale* comity analysis, the court found that: (1) the documents were "important to the litigation" and the requests were "specifically tailored" to obtain relevant documents, (2) the defendant

---

[150] *In re* Payment Card Interchange Fee & Merchant Discount Antitrust Lit., No. 05-MD-1720, 2010 WL 3420517, at *1 (E.D.N.Y Aug. 27, 2010).

[151] *Id.* at *4 (quoting Letter from Irmfried Schwimann to Visa Inc. (Aug. 11, 2009)).

[152] *Id.* at *8.

[153] *Id.* at *8.

[154] *Id.* at *9.

[155] *Id.* at *10.

[156] Devon Robotics v. DeViedma, No. 09-CV-3552, 2010 WL 3985877, at *1 (E.D. Pa. Oct. 8, 2010).

[157] *Id.* at *4.

worked largely in the United States, and much of the information sought "may very well be physically [present] in the United States at this time (e.g., on Defendant's laptop)[,]" and (3) it was "unclear whether any Italian interests would actually be undermined" by disclosure, "while nonproduction would undermine important interests of the United States."[158] Therefore, the comity factors weighed in favor of disclosure, and the court denied the defendant's protective order.[159]

C. Conflating Proportionality and Comity

Courts have at times conflated the Rule 26 discoverability and *Aérospatiale* comity analyses. For example, in *In re Rubber Chemicals*, 486 F. Supp. 2d at 1081, the court stated that Rule 26 gives the Court "discretion" to limit discovery on the grounds set forth in *Aérospatiale*. Similarly, the court in *In re Qualcomm Antitrust Litigation* held that under Rule 26, it had "'discretion to limit discovery on several grounds, including international comity,'" and then underwent the *Aérospatiale* analysis.[160]

In *In re Mercedes-Benz Emissions Litigation*, the court expressly commented on a foreign party's complaint that Rule 26's broad relevance standard is separate and distinct from the question of whether information is important to the litigation (which is the first *Aérospatiale* factor).[161] The foreign party argued that the magistrate judge "conflated" the two standards. The court appeared to agree that *Aérospatiale*'s first factor sets out a different, heightened standard than mere relevance, but suggested that if the information were "directly relevant," it is likely to be important.[162]

In *Nespresso USA, Inc. v. Williams-Sonoma, Inc.*, the court examined Williams-Sonoma's request for letters rogatory to Swiss affiliates of Nespresso. It collapsed the Rule 26 and *Aérospatiale* analyses,

---

[158] *Id.* at *4–5.

[159] *Id.* at *5–6; *see*, *e.g.*, Fenerjian v. Nong Shim Co., Ltd, No. 13CV04115WHODMR, 2016 WL 245263, at *3 (N.D. Cal. Jan. 21, 2016) (comity and foreign law alone are not dispositive when a discovery dispute arises regarding a foreign law's protection of documents sought in a United States court); Finjan, Inc. v. Zscaler, Inc., No. 17-cv-06946-JST, 2019 WL 618554, at *2 (N.D. Cal. Feb. 14, 2019). *But see*, *e.g.*, Cascade Yarns, Inc. v. Knitting Fever, Inc., No. C10-861 RSM, 2014 WL 202102, at *2 (W.D. Wash. Jan. 17, 2014) ("Use of Hague Convention procedures is particularly relevant where, as here, discovery is sought from a non-party in a foreign jurisdiction."); CE Int'l Res. Holdings, LLC v. S.A. Minerals Ltd. P'ship, No. 12-CV-08087 (CM)(SN), 2013 WL 2661037, at *8–18 (S.D.N.Y. June 12, 2013) (denying motion to compel production of documents abroad and ordering use of Hague Convention); Tiffany (NJ) LLC v. Qi Andrew, 276 F.R.D. 143, 160 (S.D.N.Y. 2011), *aff'd*, No. 10 Civ. 9471(WHP), 2011 WL 11562419 (S.D.N.Y. Nov. 14, 2011) (ordering parties to proceed through Hague Convention for discovery of non-party banks); SEC v. Stanford Int'l Bank, Ltd., 776 F. Supp. 2d 323, 341 (N.D. Tex. 2011) (directing party to proceed with discovery of foreign non-party through the Hague Convention); Pronova BioPharma Norge AS v. Teva Pharms. USA, Inc., 708 F. Supp. 2d 450, 453 (D. Del. 2010) (issuing letters of request through the Hague Convention); *In re* Rubber Chems. Antitrust Litig., 486 F. Supp. 2d 1078, 1084 (N.D. Cal. 2007) (denying motion to compel discovery on grounds of international comity).

[160] *In re* Qualcomm Antitrust Litig., No. 17-MD-02773 LHK (NC), 2018 WL 10731128, at *1 (N.D. Cal. Mar. 26, 2018) (quoting *In re Rubber Chemicals*, 486 F. Supp. 2d at 1081).

[161] *In re* Mercedes-Benz Emissions Litig., No. 16-cv-881 (KM) (ESK), 2020 WL 487288, at *6 (D.N.J. Jan. 30, 2020).

[162] *See id.* at *6 (citing Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1475 (9th Cir. 1992).

treating the latter as an enhancement of the former. "Under Rule 26, parties may seek discovery as to 'any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case . . . . Courts 'should exercise special vigilance to protect foreign litigants from the danger that unnecessary, or unduly burdensome, discovery may place them in a disadvantageous position.'"[163]

In *Hiser v. Volkswagen Group of America, Inc.*, the defendant sought to produce redacted versions of documents omitting personal information of German employees, to avoid violating German data protection law. The court considered the *Aérospatiale* factors in the Rule 26(b)(1) proportionality analysis, finding that "Plaintiffs have not shown that having the name of every individual named in every document produced is necessary, relevant, or proportional to their needs in this case, particularly when weighed against the government of Germany's important interest in protecting its citizen's privacy. Defendants may produce redacted documents."[164]

D. Consideration of Discoverability Under Rule 26, Then a Comity Analysis

Some courts have first undertaken a Rule 26(b)(1) evaluation of whether the discovery sought is permissible. Only after finding the information discoverable under Rule 26 (as both relevant and proportional), the court proceeds to an *Aérospatiale* comity analysis.

For example, in *Connex Railroad LLC v. AXA Corp. Solutions Assurance*, the court first determined that Rule 26 permitted plaintiffs to pursue the discovery at issue. Thereafter, the court concluded that the discovery would likely violate the French blocking statute, then examined the *Aérospatiale* factors to determine "[w]hether Plaintiffs may seek discovery under the FRCP or whether they must proceed in accordance with the Hague Convention . . . ."[165]

In *In re Xarelto (Rivaroxaban) Prod. Liability Litigation,* the court first concluded that Rule 26 warranted discovery. The court then determined that discovery would violate a German blocking statute, and thus concluded that it would be necessary to perform an *Aérospatiale* comity analysis.[166]

---

[163] Nespresso USA, Inc. v. Williams-Sonoma, Inc., No. 119CV4223LAPKHP, 2021 WL 942736, at *2 (S.D.N.Y. Mar. 12, 2021) (quoting Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for the S. Dist. of Iowa, 482 U.S. 522, 546).

[164] Hiser v. Volkswagen Grp. of Am., Inc., No. 5:14-CV-170-TBR-LLK, 2016 WL 11409339, at *10 (W.D. Ky. Aug. 1, 2016).

[165] Connex R.R. LLC v. AXA Corp. Sols. Assurance, No. CV1602368ODWRAOX, 2017 WL 3433542, at *12 (C.D. Cal. Feb. 22, 2017).

[166] *In re* Xarelto (Rivaroxaban) Prod. Liab. Litig., No. MDL 2592, 2016 WL 3923873, at *13 (E.D. La. July 21, 2016).

VI. RECOMMENDED APPROACH FOR U.S. COURTS APPLYING PROPORTIONALITY ANALYSIS IN A CROSS-BORDER CONTEXT

Because of the different objectives of Rule 26(b) and *Aérospatiale*'s comity analysis, this *Commentary* recommends that courts undertake a serial approach to considering scope in cross-border discovery. Ensuring that the proper scope analysis precedes a comity analysis is not only the proper legal approach, but it is a mandatory component of the case management duties at the root of Rule 26 and ultimately the dictates of Rule 1. There is no reason for parties and the court to spend time fighting over or seeking to resolve hypothetical comity issues for discovery that may not even be within scope for a particular case, because such discovery does not even meet the definition of discoverable evidence.[167]

As noted above, nothing in Rule 26(b) requires the facts around the parties' relative access to relevant information, resources, or burdens and expenses to be geographically limited to the U.S. It is immaterial *where* or *why* the specific proportionality factors attached to otherwise relevant discovery arise—only that they are fully and accurately articulated, unique to the parties, and properly balanced by the court.

First, parties and courts should consider whether the information sought is discoverable under Rule 26(b), assessing whether it is both relevant and proportional.[168] In that proportionality analysis, parties should articulate, and courts should consider, the burden on parties and non-parties in complying with the non-U.S. law, as well as the potential risk to parties and non-parties in failing to comply with the non-U.S. law. These considerations would not be an expansion of Rule 26(b)(1) nor a novel approach, but a reaffirmation of the intention behind the 2015 amendments as applied to the case before the court.[169]

---

[167] "The 2015 amendments to the Federal Rules of Civil Procedure relocated the proportionality concept to Rule 26(b)(1), making it part of the very definition of discoverable evidence." Hon. James C. Francis IV (ret.), *Good Intentions Gone Awry: Privacy as Proportionality Under Rule 26(b)(1)*, 59 SAN DIEGO L. REV. 397, 397 (2022).

[168] "So, the Court cannot endorse a simplistic holding that documents about foreign conduct are always relevant or never relevant because neither proposition is true. Instead, the analysis comes down to having a good theory of relevance. The moving party needs to explain why documents concerning foreign activities are relevant to U.S. claims or defenses, and the Court must conduct a careful analysis to determine if the foreign documents actually would be relevant." Epic Games, Inc. v. Apple Inc., No. 20-cv-05640-YGR (TSH), 2020 WL 7779017, at *1 (N.D. Cal. Dec. 31, 2020).

[169] "The burden or expense of proposed discovery should be determined in a realistic way. This includes the burden or expense of producing electronically stored information. Computer-based methods of searching such information continue to develop, particularly for cases involving large volumes of electronically stored information. Courts and parties should be willing to consider the opportunities for reducing the burden or expense of discovery as reliable means of searching electronically stored information become available." FED. R. CIV. P. 26(b)(1) advisory committee's note to 2015 amendment.

Second, if material is discoverable under Rule 26(b)(1) but subject to an ongoing transfer restriction, the parties should explore transfer under the Hague Convention before the court considers a comity analysis.

Third, assuming the first prong is met and transfer under the Hague Convention is neither an option nor viable solution, the court should then move to the *Aérospatiale* comity analysis to weigh the foreign sovereign's interests, among other factors, in deciding whether to proceed under the Rules.

A. Rule 26(b)(1) Scope Analysis, Including Proportionality, is a Threshold Inquiry

Cross-border discovery scoping inquiries should always begin with a Rule 26(b)(1) analysis of whether the information sought is nonprivileged, relevant, and proportional. In that analysis, parties should articulate, and courts should consider, not only the burdens and expenses involved in complying with both U.S. discovery and non-U.S. data privacy and protection laws, but also the unique challenges impacting the other five proportionality factors.[170] Relative access to relevant information and party resources, for example, are not as straightforward in a cross-border context as they might be with discovery located in the U.S.

The balancing test of Rule 26(b)(1) should consider the burden on parties and third parties arising from cross-border discovery. This is consistent with courts' interpretation of the "burden" prong of the Rule and the Advisory Committee notes. Both cost and noncost factors are appropriate "burdens" to consider.[171]

1. Relevancy

Relevancy as a Rule 26(b)(1) scope factor might be uniquely considered the one factor that is a true constant in the context of cross-border discovery. Relevancy is also not bounded by geography, but unlike legal privilege[172] and proportionality considerations, neither is it variable in concept. [173] It is

---

[170] Although not the direct focus of this *Commentary* in the context of examining the unique elements of cross-border discovery, compliance with U.S. privacy and data protection laws also represent a growing challenge facing U.S. discovery workflows.

[171] As elaborated above, proportionality is not limited to financial considerations. *See The Sedona Principles, Third Edition*, *supra* note 11, at 68 (Comment 2.d., addressing Sedona Principle 2, which states that "Parties should address the full range of costs of preserving, collecting, processing, reviewing, and producing ESI"); *id.* at 69 ("[T]he non-monetary costs (such as the invasion of privacy rights, risks to business and legal confidences, and risks to privileges) should be considered.").

[172] Access to information may be impacted by party affiliates or local counsel and their insistence on preventing disclosure of particular documents under local legal professional privilege standards. As detailed below during the review discussion, unique burdens and expenses associated with navigating cross-border privilege and protecting documents means privilege review workflows are more expensive.

[173] "So, the Court cannot endorse a simplistic holding that documents about foreign conduct are always relevant or never relevant because neither proposition is true. Instead, the analysis comes down to having a good theory of relevance. The moving party needs to explain why documents concerning foreign activities are relevant to U.S. claims

true as a practical matter that particular discovery can appear more or less relevant and drive fierce relevancy disagreement, but discovery scope is different from evidentiary weight. Rule 26 presents relevancy as a clear binary choice in defining scope.

What is unique in the cross-border context, however, is the challenge that requesting parties have in meeting their burden of demonstrating relevancy. Since responding party counsel is often less informed about the details of discovery stored outside the U.S., it can be difficult for requesting parties to get enough information during initial disclosures and Rule 26(f) conferences to articulate what might be very cogent relevancy arguments. Requesting party counsel is often left to review outlined information from organizational charts, corporate filings, or other preliminary discovery to support relevancy arguments.

2. Proportionality Factors

a. Importance of the discovery in resolving the issues

Although it is listed as the penultimate proportionality factor in Rule 26(b)(1), in the context of cross-border discovery's balancing act with foreign data protection laws, the importance of the discovery in resolving the issues takes on heightened importance, so we are listing it here as an initial threshold consideration after relevancy and privilege.[174] As it relates to U.S. courts and parties Rule 26(b)(1) scoping analysis, the obligations of a responding party to comply with data protection laws should not impact this particular factor. If the discovery is important to resolving the issues in the U.S. action, then it is important. Nothing should dilute that consideration.

This factor matters to a responding party's cross-border discovery efforts, however, because it will be used as part of the legal basis assessment for potential data transfers. Requesting parties who can articulate the value of cross-border discovery being sought as it connects to resolving the issues in the case can help facilitate responding party efforts. In turn, courts who must resolve motions to compel cross-border discovery that require responding parties to engage in additional work to ensure compliance with foreign data privacy laws should ensure that this factor is articulated clearly. Again, this is not because cross-border discovery requires special consideration for compliance with foreign data privacy laws in the Rule 26(b)(1) analysis but because this factor was "intended to provide the court with broader discretion to impose additional restrictions on the scope and extent of

---

or defenses, and the Court must conduct a careful analysis to determine if the foreign documents actually would be relevant." Epic Games, Inc. v. Apple Inc., No. 20-cv-05640-YGR (TSH), 2020 WL 7779017, at *1 (N.D. Cal. Dec. 31, 2020).

174 The Sedona Conference's *Primer on Social Media, Second Edition* states that "[t]he proportionality limitation on the scope of discovery includes two factors that implicate privacy concerns, i.e., 'the importance of the discovery in resolving the issues, and whether the burden . . . of the proposed discovery outweighs its likely benefit.'" The Sedona Conference*, Primer on Social Media, Second Edition*, 20 SEDONA CONF. J. 1, 27–28 (2019) [hereinafter *Primer on Social Media, Second Edition*].

discovery."[175] Requiring parties to undertake burdensome efforts for low-value discovery—wherever it is located—runs counter to both Rule 26 and Rule 1.

Responding parties also should be prepared to provide sufficient information to requesting parties to assist them with determining the importance of the discovery. As noted above, requesting parties do not have the same transparency into the actual discovery that is available in a foreign jurisdiction. While the parties may disagree over the importance of the discovery or its connection to resolving the issues in the case, responding parties do not advance proportionality arguments by failing to supplement a requesting party's knowledge base by simply stating that it's difficult to get the discovery to the U.S. Expensive disputes around cross-border discovery can be avoided with a common understanding of the likely value of the discovery.

b. Importance of the issues at stake in the action

As detailed in the Rule 26(b)(1) advisory committee's note to 2015 amendment, "monetary stakes are only one factor, to be balanced against other factors" when considering the importance of the issues at stake in the action, and "many other substantive areas also may involve litigation that seeks relatively small amounts of money, or no money at all" but seek to instead "vindicate vitally important personal or public values." This proportionality factor can be particularly challenging for parties and courts precisely because it is not always reducible to objective arguments. Parties' disagreement over the importance of the issues at stake may also go to the very heart of the merits of the case.

This factor is essential in the context of cross-border discovery since it goes directly to defining the outer limits comprising the "needs of the case." It also uniquely touches on potential privacy concerns, as the issues at stake will be balanced against the countervailing privacy interests of individuals as codified in privacy regulations like the GDPR. Thus, both requesting and responding parties should pay particular attention to Principle 2 and Principle 4 of The Sedona Conference's *Commentary on Proportionality in Electronic Discovery* when articulating discovery scope arguments. Requests for cross-border discovery should be directly connected to articulated needs of the case, with enough specific information to justify what is likely to be, at best, a less convenient source than one located within the U.S. Similarly, responding parties should consider that although they may not have a full appreciation for—or disagree with—the requesting party's articulated needs, the requesting party has very little transparency into their data sources. Responding parties should at least be prepared to explain with specificity both their knowledge of data sources located outside the U.S. and how that information ties into the requesting party's view of the importance of the issues at stake in the action.

---

[175] FED. R. CIV. P. 26 advisory committee's note to 2015 amendment (citing to the advisory committee's note to 1993 amendment).

c. Amount in controversy

As a proportionality factor, amount in controversy would seem very straightforward, helping to more concretely bound discovery scope by using an objective measure. Rule 26(a)(1)(A)(iii) requires damages computations for each claimed category of damages as part of initial disclosures, so it might be fair to assume that by the time the parties confer on cross-border discovery, they have a sense of at least a range of the amount in controversy measured by specific dollar amounts. This factor, however, also takes on heightened importance for cross-border discovery scoping because it is likely to be a heavily relied upon touchstone during Rule 26(f) conferences. Notwithstanding the above discussion of nonmonetary considerations defining the importance of the issues at stake in the litigation, a realistic and verified amount in controversy, even as an estimate, will play a large role when the parties fundamentally disagree about the issues at stake. It's one thing to request discovery that will cost a responding party a large amount when the potential damages claim is proportionally much higher or otherwise negligible but goes to "[vindicating] vitally important personal or public values."[176] It's quite another to ask for high-cost cross-border discovery to address a proportionally low-cost damages claim in a case that does not involve substantive issues beyond compensation or remuneration.

If neither the requesting nor responding parties have any concrete sense of the amount in controversy or the potential monetary costs of cross-border discovery, however, the proportionality analysis becomes even more complicated, abstract, and diluted.

d. The parties' relative access to relevant information

While the Rule 26 advisory committee note plainly states that the 2015 amendment is in part meant to address issues of "information asymmetry" and that in those cases, the "burden of responding to discovery lies heavier on the party who has more information, and properly so," cross-border discovery complicates the assumptions behind this factor—at least to the extent that it is usually directed at a responding party.[177] Responding parties should have more information about the discoverable information located outside the U.S., but it doesn't always mean that they have either the legal or practical ability to obtain it.

Organizations operating in the EU, for example, have access restrictions that are tied directly to their data protection compliance strategies. Affiliates, subsidiaries, and even parent organizations operating in the U.S. may themselves be limited by intercompany data transfer agreements executed through SCCs or Binding Corporate Rules. It is completely possible, and common, for U.S. parent organizations to be considered data processors in relation to their EU-based data controller subsidiaries. EU-based organizations may also have agreements in place with local Works Councils or employee organizations that legally limit their ability to provide U.S. colleagues access to otherwise relevant discovery.

---

[176] *Id.*

[177] *Id.*

In terms of "relative access," the above challenges certainly do not tip the balance back toward the requesting party. Responding parties would still have greater "relative access to relevant information" than requesting parties but much less relative access than discovery located in the U.S. It is incumbent on responding parties, therefore, to articulate these access challenges if they arise. Requesting parties are not in a position to understand these challenges and may fairly assume that they are not barriers to cross-border discovery unless or until requesting parties explain them. The point is not that access barriers driven by data protection and privacy compliance challenges should be used as excuses for withholding discovery, but rather that meaningful Rule 26(f) conferences cannot occur without addressing them.

Parties that in good faith apply Sedona's recommended "actual ability to obtain"[178] standard to cross-border discovery challenges will be more likely to streamline necessary discovery and avoid costly discovery disputes over disproportionate information.

e. Parties' resources

As noted above, responding parties may not always be able to leverage the resources attributed to them when working on cross-border discovery. This does not mean that this factor should be considered differently when determining whether cross-border discovery is within scope. It is simply another reminder of the heightened importance of both requesting and responding parties sharing information during Rule 26(f) conferences related to cross-border discovery. In general, it serves the interests of both parties and the court to ensure that everyone has a full picture of the true practical ability of the parties to leverage their available resources.

f. Burden or Expense

i. Privacy, Cost, and Noncost Factors in Cross-Border Discovery

Some courts have recognized the privacy interests of parties and non-parties in the Rule 26(b)(1) proportionality analysis under specific U.S. legal or regulatory provisions or common law considerations. It would be appropriate for parties to articulate, and for courts to consider, similar privacy interests of non-U.S. residents, particularly those that are codified under local laws or regulations and directly impact the burden element of a proportionality analysis but do not lend themselves to a mathematical financial calculation.[179]

---

[178] The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody or Control."* 25 SEDONA CONF. J. 1, 11 (forthcoming 2024).

[179] The Sedona Conference's *Primer on Social Media, Second Edition* states that "[t]he proportionality limitation on the scope of discovery includes two factors that implicate privacy concerns, i.e., "the importance of the discovery in resolving the issues, and whether the burden . . . of the proposed discovery outweighs its likely benefit." *Primer on Social Media, Second Edition*, *supra* note 174, at 27–28.

For example, in *Johnson v. Nyack Hospital*, 169 F.R.D. 550, 562 (S.D.N.Y. 1996), the court held that Rule 26 allows courts to limit discovery on account of burden, including "where the burden is not measured in the time or expense required to respond to requested discovery, but lies instead in the adverse consequences of the disclosure of sensitive, albeit unprivileged, material," and that courts should consider "the burdens imposed on the [responding parties]' privacy and other interests."[180]

In *Henson v. Turn*, the court considered the defendant's requests for inspection or complete forensic images of mobile devices. The plaintiffs argued that those requests were overbroad and invaded their privacy rights. The court held that while questions of proportionality often arise in the context of disputes about the expense of discovery, proportionality is not limited to such financial considerations.[181] Courts and commentators have recognized that privacy interests can be a consideration in evaluating proportionality, particularly in the context of a request to inspect personal electronic devices.[182]

Some commentators have argued that privacy should not be considered an element of the proportionality analysis—especially as a noncost factor—and that in fact, both discovery law and privacy protection would be better served by a continued reliance on the "good cause" framework of Rule 26(c).[183]

---

[180] 169 F.R.D. 550, 562 (S.D.N.Y. 1996). According to Robert D. Keeling and Ray Mangum, proportionality in discovery is particularly relevant at a time when the protection of privacy is of increasing concern in the United States and abroad. Robert D. Keeling & Ray Mangum, *The Burden of Privacy in Discovery*, 20 SEDONA CONF. J. 415, 416 (2019). "The burden of privacy is distinct and independent from the expense of litigation, and the risks to privacy are felt primarily after, rather than before, production." *Id.* at 440 (footnote omitted). *See also* Rivera v. NIBCO, Inc., 364 F.3d 1057, 1065 (9th Cir. 2004) (affirming district court's refusal to allow discovery into certain private information of plaintiffs in a Title VII employment case because, among other things, "[t]he chilling effect such discovery could have on the bringing of civil rights actions unacceptably burdens the public interest"); Wiesenberger v. W.E. Hutton & Co., 35 F.R.D. 556, 557 (S.D.N.Y. 1964) (limiting the disclosure of personal income tax returns unless "clearly required in the interests of justice"); Conn. Importing Co. v. Cont'l Distilling Corp., 1 F.R.D. 190, 193 (D. Conn. 1940) (recognizing that the court has discretion to limit discovery requests to avoid an undue invasion of privacy); Appler v. Mead Johnson & Co., No. 3:14-cv-166-RLY-WGH, 2015 WL 5615038, at *6 (S.D. Ind. Sept. 24, 2015) (declining to compel the production of entire categories of data from a Facebook profile due to the privacy burden outweighing the relevance to the case).

[181] *Henson v. Turn*, No. 15-cv-01497-JSW (LB), 2018 WL 5281629, at *4 (N.D. Cal. Oct. 22, 2018).

[182] *See* Hespe v. City of Chicago, No. 13 C 7998, 2016 WL 7240754, at *3 (N.D. Ill. Dec. 15, 2016) (affirming order denying request to inspect plaintiff's personal computer and cell phone because, among other things, inspection "is not 'proportional to the needs of this case' because any benefit the inspection might provide is 'outweighed by plaintiff's privacy and confidentiality interests'"); *In re* Anthem, Inc. Data Breach Litig., No. 15-md-02617 LHK (NC), 2016 WL 11505231, at *1–2 (N.D. Cal. Apr. 8, 2016) (denying request to inspect or forensically image plaintiffs' computers, tablets and smartphones as "invad[ing] plaintiffs' privacy interests" and "disproportional to the needs of the case.").

[183] "We think the correct path is not to try to retrofit privacy into proportionality, but to take the subject head on and see what happens." Lee H. Rosenthal & Steven S. Gensler, *The Privacy Protection Hook in the Federal Rules*, 105 JUDICATURE 77, 81 (2021). "Rule 26(c), then, provides a well-established framework for the protection of privacy rights in discovery, a framework that has been recognized by the Supreme Court and long utilized by the lower courts." Francis, *supra* note 167, at 409.

> A party or any person from whom discovery is sought may move for a **protective order** in the court where the action is pending—or as an alternative on matters relating to a deposition, in the court for the district where the deposition will be taken. The motion must include **a certification that the movant has in good faith conferred or attempted to confer** with other affected parties in an effort to resolve the dispute without court action. The court may, **for good cause**, issue an order **to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense** . . . .
>
> FED. R. CIV. P. 26(c) (emphasis added).

The arguments against considering privacy as a proportionality element generally, and as a noncost factor specifically, include: privacy is a separate consideration from proportionality; proportionality should focus on economic costs;[184] Rule 26(c) is more flexible and lends itself to more consistent and transparent decision-making;[185] privacy could have been included in the 2015 amendments to Rule 26(b) but was not;[186] and consideration of privacy as an element of the proportionality analysis could actually dilute privacy protections.[187] As Hon. James C. Francis IV (ret.) points out, *Henson* and cases like it "speak of privacy as a proportionality factor but do not engage in anything approaching a complete proportionality analysis under Rule 26(b)(1)."[188]

Robert Keeling and Ray Mangum, on the other hand, recognize that courts still have a tendency to focus on cost factors in proportionality but argue that the 2015 amendments have led more and more courts to attempt to integrate privacy in the proportionality analysis.[189] They point out that the

---

[184] Privacy considerations "should be limited to circumstances in which the need to preserve privacy interests generates the kind of financial cost and burden that is properly within the scope of Rule 26(b)(1). Francis*, supra* note 167, at 400.

[185] Rosenthal & Gensler, *supra* note 183, at 78–79; *see generally* Francis*, supra* note 167.

[186] "It is true that the term 'burden' is open-ended and captures noneconomic concerns. But we struggle to accept the idea that the Advisory Committee interjected privacy into the proportionality calculus (and therefore into the scope of discovery) without using the word privacy in the rule text or the committee notes[.]" Rosenthal & Gensler, *supra* note 183, at 80.

[187] "[T]reating privacy as a proportionality factor may actually threaten to devalue privacy interests. This is because considering privacy and economic factors together suggests that if the cost of the requested discovery were less, then the discovery might be allowed, notwithstanding the impact on privacy. Only if the economic costs are zero, or if they are not considered as a factor alongside privacy, does the value assigned to privacy interests in a particular case become apparent." Francis, *supra* note 167, at 426.

[188] *Id.* at 417.

[189] "Even today, it remains common, among both the bench and the bar, to think of proportionality in discovery as relating primarily to financial burdens. With the re-emphasis on proportionality brought about by the 2015 amendments and the growing public debate over the importance of privacy, however, there has been a clear trend by courts and commentators toward recognition of privacy interests as an integral part of the proportionality analysis required by Rule 26(b)(1)." Keeling & Mangum, *supra* note 180, at 426–27.

Rule 34 (a)(1) advisory committee notes to the 2006 amendment specifically address "issues of burden and intrusiveness," including "confidentiality and privacy," by suggesting that courts can look to either Rule 26(c) or Rule 26(b)(2), and that an "important assumption in this directive was the advisory committee's intent that the burden of privacy should be considered in setting the scope of discovery."[190]

This *Commentary* does not attempt here to resolve the question of whether privacy is or should be considered as its own factor in Rule 26(b) but simply recognize the reality that in cross-border discovery, for both parties and non-parties, there are burdens and risks associated with privacy concerns as reflected in non-U.S. data protection laws. Some of those burdens are measurable and expensive, and others cannot easily be reduced to specific dollar amounts or metrics but are very real. Addressing compliance with data protection obligations is a legitimate cost and noncost burden, apart from the specific "privacy" rights of any given individual.

ii. Cost Factors

Legal data privacy and labor law assessments for every processing step (identification, preservation, collection, processing, review, and production) are necessary. Each step requires a legal basis according to GDPR. Article 6 of the GDPR, for example, requires balancing the interests of the controller (producing party) and the individual/data subject (employees). This balancing (explaining why the interests of the controller outweigh the interests or fundamental rights and freedoms of the data subject) needs to be done properly for each discovery task representing an additional data processing step and for each production resulting in a third-country data transfer under the GDPR. The producing party must document every step and assessment thoroughly and invest additional billable hours to do so.

Article 88 of the GDPR also allows member states to enact more specific rules for processing employees' personal data in the employment context. In addition to the data privacy assessment according to GDPR, local data privacy laws need to be checked.

(a) Identification

In Europe, there are obligations toward the data subject/individual regarding collecting and processing his data.[191] The controller needs to inform the data subject/individual that his data will be processed,[192] e.g., "the identity and the contact details of the controller," "the purposes of the processing for which the personal data are intended as well as the legal basis for the processing," "where

---

[190] *Id.* at 424.

[191] *See* GDPR, *supra* note 52, arts. 13, 14 ("Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information . . . .").

[192] *Id.* art. 13(1)–(2).

the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party."

Identifying relevant cross-border discovery outside the U.S. is often more expensive than executing those same identification tasks in the U.S.

Requesting parties who believe relevant discovery is located outside the U.S. may have to engage their counsel and investigative teams in additional hours to confirm their belief prior to issuing a cross-border discovery request. Information governance and management policies may be impacted in jurisdictions with data protection regulations as part of the controller's data protection and privacy compliance strategy. As a result, U.S.-based legal teams may be restricted from accessing data sources located in these jurisdictions.[193] Responding parties may generate larger than average vendor and law firm invoices working to identify more convenient U.S. sources of discovery that contain the same information the requesting party is seeking without the attendant cross-border data protection risks.

Common identification tasks like custodial interviews or questionnaires require additional time to customize, translate, and negotiate. In-house legal teams working to identify relevant cross-border discovery may have to travel, along with their outside counsel/vendors, to engage in additional meetings to investigate potentially relevant data sources in other jurisdictions, and potentially implement additional security measures (such as SCCs) to access the data.

While parties are working to identify relevant cross-border discovery, outside counsel is often engaged in more frequent Rule 26(f) conferences regarding whether to phase discovery. Even if both requesting and responding parties agree to a phased approach in which data from foreign sources is deprioritized in favor of more convenient U.S. data sources—or generally any data not subject to data protection laws—shaping the details of the phased approach takes time. Counsel for both parties must engage in additional hours to ensure they are being thorough in their search for relevant information, analyzing initial disclosures and information provided by opposing parties regarding the potential location of relevant discovery and spending time crafting strategic approaches to phased discovery that minimize their client's data protection exposure.[194]

The prior-notice obligation can further frustrate identification efforts if data subjects have incentive to destroy information and is complicated by its practical limitation to known custodians or data subjects.

---

[193] Jeff Griffiths, *5 Questions About Cross-Border Discovery*, DELOITTE, https://www2.deloitte.com/us/en/pages/advisory/articles/five-questions-cross-border-discovery.html (last visited June 12, 2024).

[194] *International Litigation Principles*, *supra* note 2, at 16.

(b) Preservation

As noted in the preamble to 'The Sedona Conference's *Commentary on Managing International Legal Holds*, parties "in actual or anticipated cross-border litigation face a conundrum. On one hand, they are often required to comply with strict requirements for the preservation of discoverable data. On the other, privacy laws and regulations can severely restrict their legal ability to preserve personal data."[195]

In Europe, there are obligations towards the data subject/individual impacting preservation efforts.[196] The controller needs to inform the data subject/individual that his data will be processed,[197] e.g., "the identity and the contact details of the controller," "the purposes of the processing for which the personal data are intended as well as the legal basis for the processing," "where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party."

In their effort to navigate these restrictions and still comply with U.S. obligations to preserve data, responding parties will have to invest additional time and cost in a host of additional tasks unique to cross-border discovery:

- educating, if not training, U.S. legal teams to ensure preservation activities comply with data protection laws
- educating legal teams outside the U.S. on what preservation obligations are
- first considering, then aligning on, and finally documenting the lawful basis for preserving data
- creating customized and case-specific legal-hold notices with language aimed at providing not only comprehensive legal-hold instructions but sufficient notice in compliance with local data protection laws; translating legal-hold notices into local languages
- engaging local and data privacy counsel as well as an organization's data protection officer
- engaging a local labor expert or informing local human resources officials to discuss if, e.g., Works Council needs to be involved, and if yes, informing Works Council
- allocating additional time to analyze identified data sources to ensure data minimization in application of any technical legal holds

---

[195] *Commentary on Managing International Legal Holds*, *supra* note 10, at 166.

[196] *See* GDPR, *supra* note 52, arts. 13, 14 ("Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information . . . .").

[197] *Id.*, art. 13(1)–(2).

- training local resources and potentially onboarding new technology to prevent unnecessary or unapproved cross-border transfers of data or processing when using U.S.-based legal technology to place technical legal holds on non-U.S. data sources
- implementing additional legal-hold management tasks associated with time-sensitive scoping updates and releasing custodians and data from legal holds as soon as the data is no longer "necessary for the purposes for which the personal data is processed"[198]

Some of the above tasks may require a responding party to hire new employees or consultants. Even if many of the above tasks are completed by existing employees and responding parties do not invest in additional human or legal technology resources, the tasks are often done at the direction or advice of outside counsel.

(c) Collection

Bringing about targeted collections as outlined by the identification efforts involves more cost and time in cross-border cases. Parties will need to focus on using filters, keywords, and extended early data assessments[199] to ensure targeted collection efforts comply with data minimization requirements. In addition, restricted access might mean multiple teams working together to advise on both U.S. discovery and non-U.S. data protection obligations, and non-U.S. technology staff generally will be less familiar with U.S.-style collection efforts.

(d) Review

Cross-border document reviews are inherently more expensive than the average U.S.-based document review—or any review involving discovery from a single jurisdiction.

Prior to engaging the review, a responding party will have to take additional steps during processing, early case or data assessments, and culling to minimize data sets down to only what is necessary for the purposes of the case. It may also be necessary to create multiple review databases to facilitate in-country review and then work to coordinate de-duplication efforts across data sets from both the U.S. and non-U.S. workspaces. These steps can increase vendor costs before a review even starts.

Determining whether the information at issue is subject to a recognized legal privilege may create additional burdens. As noted in The Sedona Conference's *Commentary on Cross-Border Privilege Issues*, "multijurisdictional conflicts (and their attendant privilege issues) are becoming more common" and uniquely impact cross-border discovery by adding additional dimensions to privilege considerations, including: balancing varied privilege and disclosure standards across document collections; hedging against increased waiver risk and compelled disclosure; and protecting against cross-matter and

---

[198] *Commentary on Managing International Legal Holds*, *supra* note 10, at 213 (citing to GDPR, *supra* note 52, art. 5(1)(e)).

[199] Early data assessments typically involved using data analytics and advanced eDiscovery filtering techniques to understand the contents of electronic data at the outset of a matter, often as the first step in an early case assessment.

jurisdictional requests for production sets that might subject documents to different privilege protections than those they were analyzed for during their original production.[200] Accordingly, privilege review is more complex and often more costly when reviewing documents from multiple jurisdictions. Reviewers must be trained in cross-border legal privilege considerations and varying standards of legal privilege as well as applicable data privacy and protection laws. EU-qualified outside counsel may need to be employed to both ensure the process is protected by legal privilege and that the document review effort correctly applies local legal privilege standards in their analysis. Variations and limitations on in-house counsel legal privilege along with jurisdictional choice-of-law approaches mean outside counsel specializing in cross-border privilege law may have to be involved.[201]

The personal data being transferred must be restricted to the absolute minimum necessary for the litigation. This results from the principle of data minimization defined in GDPR Article 5(1)(c) (personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed") and applied in GDPR Article 9 (prohibiting processing of special categories of personal data). Therefore, first-level review and data privacy and protection review may need to be conducted locally in Europe.[202] It is not just a relevancy review but a review to detect personal information (e.g., name, email, phone number), private or sensitive personal content (e.g., holidays, sickness, parental leave) and Works Council related topics. This additional content then needs to be redacted unless (1) it is necessary for some reason to a claim or defense and (2) the interests of the producing party outweigh the interests of the individuals/data subjects. Then, only the relevant data that is necessary for the legal defense will be transferred to the U.S. If local review is required, it often is more expensive than U.S.-based document review resources. It may also be necessary to create a specific security architecture for review of non-U.S. documents as part of an organization's data privacy and protection strategy and commitments.

Additional quality control measures and per-document review costs increase as document reviewers balance U.S. and non-U.S. obligations and analysis. First-level reviewers take more time to ensure compliance with both U.S. and non-U.S. laws, checking and double-checking their analysis. Second-level reviewers take more time engaging in quality control because the consequences of failing to properly account for, redact, or analyze personal information and multiple legal privilege standards are heavier. The pace of document review typically slows down, and overall review budgets increase. Increased redaction work might be necessary to ensure data privacy compliance. Language translation tools may also need to be employed, along with document reviewers with proficiencies in other languages and higher per-hour billable rates.

---

200 *Commentary on Cross-Border Privilege Issues*, *supra* note 9, at 483.

201 *Id.* at 507–32.

202 Article 29 Data Protection Working Party, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation, at 11 (Feb 11, 2009), *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf; *International Litigation Principles*, *supra* note 2, at 18 n.56.

Technology-assisted review (TAR) can help with the pace of document review and minimizing data sets for manual review. TAR itself, however, often represents a "processing" of personal information under data protection laws and may require additional outside counsel consultation and guidance to engage a data impact or risk assessment.

(e) Production

Increased production costs associated with cross-border discovery center on ensuring adequate security and protection of documents produced to requesting parties in the U.S. and begin long before document productions start.

Requesting and responding party counsel may spend additional time negotiating pretrial stipulations, orders, and protocols that are designed to account for foreign data protection laws. Protective orders in cross-border cases often contain additional provisions: detailing the foreign data protection law; restrictions on copying and utilizing the discovery only for the case at issue; limiting the use of sensitive information; allowing for redaction of nonrelevant personal information within otherwise responsive documents; outlining unique or additional confidentiality classifications; disposing of discovery and certifying such disposition and destruction within a specific time period; and allowing for time in scheduling orders to carry out a data protection legitimization plan that documents the responding party's compliance with foreign data protection laws.[203]

ESI protocols drafted for cross-border discovery also require additional billable hours from counsel for both parties. The protocols may incorporate some of the above listed concerns but also focus specifically on formatting agreements that minimize the risk of noncompliance with data protection laws by: allowing for alternative or non-native formats; restricted metadata provisions; supplemented metadata provisions aimed at optimizing tracking and control of cross-border discovery; unique or duplicative Bates stamping connected to foreign data sets; redaction provisions customized for data privacy; and security transfer protocols and methods.

To resolve the conflict between the requirements of the GDPR and U.S. discovery requests, EU authorities have developed a "layered" approach to document productions.[204] This means "[a]s a first step, there should be a careful assessment of whether anonymized data would be sufficient in the particular case. If this is not the case, then transfer of pseudonymized data could be considered. If it is necessary to send personal data to a third country, its relevance to the particular matter should be assessed before the transfer—to ensure that only personal data that is actually necessary is transferred and disclosed."[205] Anonymization and pseudonymization are expensive.

---

[203] *International Litigation Principles*, *supra* note 2, at 20–21.

[204] EDPB Guidelines 2/2018 on derogations of Article 49, *supra* note 92, at 12.

[205] *Id.*

Production of data means transferring the data to the U.S. A legal basis for transferring personal data to the U.S. is required. A specific assessment is needed to determine whether the transfer is necessary for the legal defense (balancing of interests of controller and individual/data subject).[206] Assessing if a data transfer should be discussed with local data protection authorities increases production costs. If local data protection authorities should be involved, these meetings will involve additional assessments. Meetings with the data protection authorities will be time-consuming.

When data is transferred to the U.S., the custodians and every data subject/individual whose name appears in the production set need to be informed.[207] . Depending on the amount of data in the production set, this could mean that several thousand individuals must be informed each time there is a production. Any violation of Article 6, 13 or 49 of the GDPR can result in severe fines and civil liability.

Some countries outside the EU consider their data as confidential, so a transfer outside those countries is not possible without the approval of their authorities in charge. For example, China: under Article 36 of the Data Security Law of the People's Republic of China (which came into effect on September 1, 2021), "the competent authority of the People's Republic of China shall process a request for data from a foreign judicial or law enforcement authority in accordance with relevant laws and international treaties and agreements entered into or acceded to by the People's Republic of China, or under the principle of equality and reciprocity. Without the approval of the competent authority of the People's Republic of China, a domestic organization or individual shall not provide data stored in the territory of the People's Republic of China to any foreign judicial or law enforcement authority."

Vendor costs associated with implementing the above ESI protocol and protective order provisions are also usually more expensive in cross-border cases. Vendors may have to switch to a new secure transfer technology and modify their existing workflows to ensure compliance. Additional technical safeguards around not only transferring but accessing production sets may increase costs. As noted above, additional costs associated with cross-referencing review sets may also drive increased production quality-control costs. Vendors spend more time coordinating production sets, double-checking for duplicate documents, and refreshing or overlaying metadata fields to ensure requesting parties receive sufficient transparency into data sources.

(f) Attorney and Vendor Fees

Many drivers behind increased attorney and vendor fees are detailed above. It is important to note, however, that even if a particular driver is not a factor on a given matter, cross-border discovery generally costs more in attorney and vendor fees. Discovery, disclosure, data protection and privacy

---

[206] GDPR, *supra* note 52, art. 49(e)(1).

[207] *Id.* arts. 13, 14 (see examples above, and in addition, "where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission . . . .").

laws, and labor laws from multiple jurisdictions are necessarily involved. This alone results in increased billable hours that can impact both responding and requesting parties.

In the EU context, SCCs can be used as a ground for data transfers from the EU to third countries to ensure appropriate data protection safeguards under the GDPR.[208] When U.S. outside counsel and vendors are involved, SCCs may be required to ensure that counsel and vendors can investigate and review the data (accessing the data from the U.S. via a review tool in Europe is already a transfer of personal data to the U.S.). SCCs take time and result in additional meetings between clients, vendors, and outside counsel. As counsel and vendors work with their own technical resources and consult data privacy counsel and/or data protection officers to establish sufficient technical and organizational measures, the cost of basic engagement increases. Completing Transfer Impact Assessments can further drive counsel and vendor engagement costs upward.[209]

iii. Noncost Factors

Expanding on the discussion regarding cost factors, parties and non-parties may also experience:

- Variations in discovery and privacy compliance workflow skill sets between U.S. and non-U.S. vendors and partners.
- Varied data protection and privacy strategies across clients, counsel, and vendors.
- Legal technology variations and limitations associated with different global markets or availability within a particular data protection compliance strategy.
- The need to educate foreign vendors on U.S. discovery obligations.
- The need to educate U.S. vendors on foreign data protection and privacy obligations.
- Resistance from subsidiary or parent companies to broad discovery cooperation that may frustrate U.S. legal analysis and assumptions around possession/custody/control standards.
- Organizational change management associated with reconciling different discovery and disclosure practices or scope expectations.
- Adapting discovery workflows to include consultation with data.
- General cultural, language and communication differences.
- Reputational damage and risk management concerns associated with noncompliance with data protection laws.

---

[208] *Standard Contractual Clauses (SCC)*, EUROPEAN COMM'N, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (last visited June 12, 2024).

[209] David Rosenthal, *Transfer Impact Assessment Templates*, "IAPP (Sept. 1, 2021), https ://iapp.org/resources/article/transfer-impact-assessment-templates/.

- Potential fines or criminal liability.
- Impact on organizational and employee dynamics, especially for non-U.S. employees living in jurisdictions with minimal discovery activity but data protection laws that consider privacy a fundamental right.

One of the largest noncost factors impacting cross-border discovery is simply regulatory uncertainty. Data protection laws are in a constant state of flux around the world. Even in jurisdictions like the EU where the GDPR has been in place for years, there is still uncertainty around data transfers. As noted above, the July 2023 adequacy decision by the European Commission means that U.S. organizations can use the EU-U.S. Data Privacy Framework ("DPF") to transfer personal information. That said, companies with Privacy Shield experience know all too well that an adequacy decision in this context is a preamble to challenges in the European Court of Justice by data protection advocates. This means U.S. organizations interested in participating in the Framework are faced not only with a refresh of their internal operations to ensure compliance with the DPF, but they are also faced with uncertainty around the DPF's long-term viability and particular utilization for implementing cross-border discovery.

None of these factors—unlike privacy redactions, for example—are easily reduced to dollar amounts or numbers, but they nevertheless are burdens associated with cross-border discovery.

While it may be true that there is a dearth of cross-border case law reflecting parties and courts properly considering privacy and proportionality under Rule 26(b), it is also true that some challenges driving the above factors are new. The GDPR, for example, post-dates the 2015 amendments, as does the reality that an accelerated amount of relevant discovery is being stored in cloud-based applications and servers that do not reside in the U.S. Thus, parties and courts involved in cross-border discovery are still adapting to a world in which more and more of the relevant, nonprivileged discovery resides outside the U.S. and is subject to jurisdictional data privacy and protection scrutiny. Because this is the new reality, parties should at least articulate and courts should consider noncost factors as part of the Rule 26(b)(1) proportionality analysis to the extent that they present as actual burdens on the discovery process.[210] This is important whether an argument is made for protection of privacy as a right in the discovery process.

---

[210] "Businesses continue to transcend national borders at unprecedented rates. As a result, it is increasingly rare to represent a purely 'domestic' corporate client. At the same time, foreign data privacy laws and other blocking statues that prohibit the wholesale transfer of foreign documents to the United States are proliferating on a global basis. The result is a 'catch-22' pitting domestic discovery obligations against foreign data transfer restrictions." E-Discovery Working Group, *Cross-Border E-Discovery: Navigating Foreign Data Privacy Laws and Blocking Statutes in U.S. Litigation*, N.Y.C. BAR (Reissued February 2020), https://www.nycbar.org/reports/cross-border-e-discovery-navigating-foreign-data-privacy-laws-and-blocking-statutes-in-u-s-litigation/.

B. If material is discoverable under Rule 26(b)(1) but subject to an ongoing transfer restriction, the parties should explore transfer under the Hague Convention before the court considers a comity analysis

Ideally, the proportionality assessment is conducted and agreed to by the parties and avoids a discovery dispute involving U.S. courts. If necessary, the court may need to resolve a dispute and rule on the scoping arguments. As recommended throughout this *Commentary*, the proportionality analysis and discoverability rulings should initially be limited to scope questions and avoid unnecessary questions of comity or conflict of laws.

If the discovery is proportional under Rule 26(b)(1) and can be transferred to the U.S. without placing a party in danger of violating non-U.S. data protection laws, then the responding party should work to process and transfer the information to the requesting party. There may be instances, however, in which responding parties are still restrained from processing and/or transferring necessary and proportional discovery based on the laws of the jurisdiction in which the discovery is stored—despite an agreement, stipulation, or U.S. court order. When faced with transfer restrictions regarding proportional discovery, such as blocking statutes, this *Commentary* recommends that the parties consider transfer under Chapter II of the Hague Convention and that courts withhold ruling on comity or conflict-of-laws issues until a Chapter II solution is explored.[211]

---

[211] Although recent cases like *In re Procom Am., LLC*, 638 B.R. 634, 646 (Bankr. M.D. Fla. 2022) have served as reminders that *Aérospatiale* rejected the Hague Convention as the exclusive means of obtaining evidence abroad, the Supreme Court also confirmed that the "the text of the Evidence Convention, as well as the history of its proposal and ratification by the United States, unambiguously supports the conclusion that it was intended to establish optional procedures that would facilitate the taking of evidence abroad." Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for the S. Dist. of Iowa, 482 U.S. 522, 538 (1987). In concurring in part and dissenting in part, Justice Blackmun added:

> "In my view, the Convention provides effective discovery procedures that largely eliminate the conflicts between United States and foreign law on evidence gathering. I therefore would apply a general presumption that, in most cases, courts should resort first to the Convention procedures. An individualized analysis of the circumstances of a particular case is appropriate only when it appears that it would be futile to employ the Convention or when its procedures prove to be unhelpful." *Id.* at 548–49.

Justices Blackmun, Brennan, Marshall and O'Connor were concerned that the majority opinion ignored the importance of the Hague Convention by characterizing it as optional, risking case-by-case comity analysis and overutilization of the Rules to order cross-border discovery. *Id.* at 548

As noted above, not all Hague Convention Member States adhere to all provisions of Chapter II. Parties should first consult the Convention's *Table Reflecting Applicability of Articles 15, 16, 17, 18 and 23 of the Hague Evidence Convention* before working on a Chapter II solution involving diplomatic officers, consular agents, or commissioners. However, in outlining a serial analysis that moves from scope as defined under Rule 26(b)(1) to consideration of Chapter II of the Convention before digging into a comity analysis, this *Commentary* believes it is both adhering to *Aérospatiale* and directly addressing the problem Justice Blackmun outlined. *See* Hague Conference on Priv. Int'l Law [HCCH], Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters: Table Reflecting Applicability of Articles 15, 16, 17, 18 and 23 of the Hague Evidence Convention (June 2017), https://assets.hcch.net/docs/627a201b-6c7a-4dc2-86ad-c1da582447d4.pdf (last visited June 12, 2024).

Although this *Commentary* recommends that parties facing transfer restrictions impacting necessary and proportional discovery explore transfer through the appointment of a Commissioner under Chapter II of the Hague Convention, it also recommends that this option only be engaged when the parties are in agreement, or when the responding party can otherwise leverage a Chapter II request without triggering a prolonged discovery dispute.

C. If the parties do not agree to the use of Chapter II of the Hague Convention, courts should then move to *Aérospatiale* inquiry

Rule 26(b)(1) defines the "Scope in General" for civil discovery in the U.S. The 2015 amendments provide clarifying language that explicitly includes the principle of proportionality as part of the very definition of what is discoverable. The amendments include neither explicit references to privacy nor prohibitions against burden or expense consideration associated with data protection or privacy compliance. The amendments also do not contain geographic or jurisdictional limiters associated with the location of the relevant, nonprivileged discovery. Nowhere in Rule 26(b) does it reference discovery scope and its limits being tied only to considerations of discovery located in the U.S. Perhaps most importantly, Rule 26(b) does not address the interests of foreign sovereigns, conflicts of

---

While the Chapter I Letters of Request system is available, the reality of discovery timetables in U.S. civil procedure can make it difficult to employ this method. Either both parties would have to agree or one party would have to alone first petition the U.S. court to issue Letters of Request as the judicial authority in the Requesting State. In addition to basic elements regarding the judicial authority, and the parties' names and addresses, the Letters must detail: the nature and status of the proceedings, including a summary of the complaints, defenses, and counterclaims; a clear and definite statement about the evidence sought, including how specifically the evidence relates to the proceedings in the Requesting State and specific identification of the documents—especially if the Requested State has made a declaration under Article 23 and does not recognize the Convention for pre-trial discovery requests. *See* HAGUE CONFERENCE ON PRIV. INT'L LAW, PRACTICAL HANDBOOK ON THE OPERATION OF THE EVIDENCE CONVENTION, at 43–136 '(4th ed. 2020). The U.S. court would then have to issue the Letters to the Central Authority in the Requested State and wait for a response, which is dependent on the Requested State's designated judicial authority procedures and docket.

The Convention itself does not define Consul or Commissioner under Chapter II but instead leaves it to the State of Origin to define under its own laws who can serve as Consul or Commissioner unless the State of Execution has specific laws that must be followed. Again, as a practical matter, reliance on diplomatic officers or consular agents to serve as Consul could face logistical challenges. While a request must still be made for a Commissioner to be appointed, and the permission is dependent on the decision of the competent authority designated by the State of Execution, requests are generally processed faster and permission can be given both generally and on a case-by-case basis. *Id.* at 137–146.

France, for example, recently required a one-month reporting period for its Strategic Information and Economic Security Service authority to report on requests for information or documents falling under its blocking statute through the Ministry of the Economy & Finance. *See* Décret 2022-207 du 18 février 2022 relatif à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères [Decree 2022-207 of Feb. 18, 2022 relating to the communication of economic, commercial, industrial, financial or technical documents and information to foreign natural or legal persons], Journal Officiel de laRépublique Française [J.O.] [Official Gazette of France], Feb. 20, 2022, p. 14. While France may be focused on reporting requests for information and documents as part of the enforcement mechanisms of its workflows, it is also serving as an example of the potential expediency of Chapter II requests.

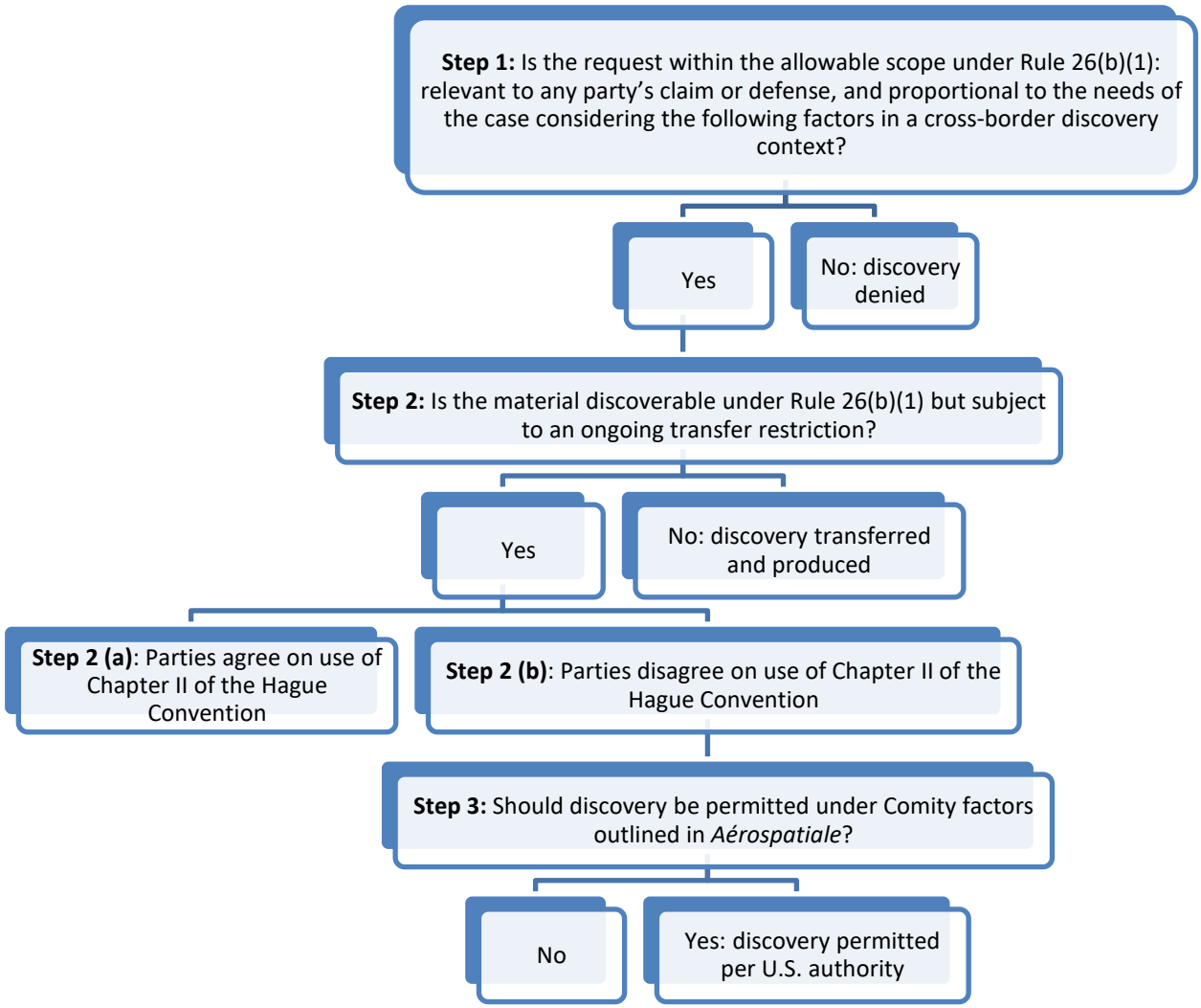
law, or comity issues. It doesn't need to. The scope definition includes considerations sufficient to guide parties and the court in determining proper scope involving cross-border discovery. A Rule 26(b) analysis alone is neither necessary nor sufficient to address the broader considerations of foreign sovereigns and resolve actual conflicts of law. If discovery is outside the scope of Rule 26(b), then there is no conflict to address.

In contrast, the comity analysis outlined in *Aérospatiale* is specifically intended to address the interests of foreign sovereigns, which are generally not represented in the litigation. These principles are particularly important when the rights of foreign data subjects are at issue, as they are when cross-border discovery implicates, for example, the rights of non-U.S. employees or residents under foreign data protection laws. Foreign jurisdictions and individuals are not present in the U.S. and usually not able to make arguments to protect their rights. Their interests may not fully align with those of the parties to the litigation. Accordingly, courts must be diligent in applying the *Aérospatiale* analysis not for the purpose of managing their dockets, but respecting these important interests of nations and individuals not present in their courtrooms. For these reasons, the comity analysis has a very different focus than the Rule 26(b)(1) analysis, and it is essential not to confuse or conflate the two.

Only if the court determines that the requested documents are discoverable under Rule 26(b)(1) should the court turn its attention to the elements of a comity analysis under *Aérospatiale*.

D. Recommended Flowchart

The following flowchart reflects this serial approach to considering potential foreign law conflict issues in cross-border discovery.



Each of the comity factors outlined above are discussed in Section VI of this *Commentary*.

VII. PRACTICE POINTS FOR ADDRESSING PROPORTIONALITY IN CROSS-BORDER DISCOVERY

Practice Point 1: Cross-border proportionality analysis for U.S. discovery obligations should proceed as the collective responsibility of the parties and the court to consider the unique importance and benefit of the discovery sought as well as the specific burden and expense involved in obtaining and disclosing the relevant information.

1. Responding parties should remember that requesting parties do not have transparency into the data protection requirements associated with discovery requests for information located outside the U.S. and should consider informing requesting parties of the specific burden and expense involved in obtaining and disclosing relevant information as early as possible.

    a. Parties should be prepared to describe relevant non-U.S. discovery sources in their possession, custody. or control, including relevant documents, ESI, and data sources they may produce to support their claims or defenses, as part of their Rule 26(a)(1)(A)(ii) initial disclosure obligations, and to supplement disclosures as they learn about additional sources.

    b. Parties should be prepared to identify known burdens or challenges regarding the identification, preservation, collection, review, or production of relevant non-U.S. information, including any related privacy or data protection compliance obligations, as part of their Rule 26(f)(2) conference responsibilities.

    c. Parties should be prepared to state their views and proposals on the discoverability and proportionality of relevant information located outside the U.S., including the specific burdens and expenses associated with related privacy or data protection obligations and whether the information at issue is unreasonably cumulative, duplicative, or can be obtained from more convenient, less burdensome, or less expensive sources, as part of their Rule 26(f)(3) discovery plan obligations.

2. Requesting parties should be prepared to articulate the unique importance and benefit of discovery sought from non-U.S. sources as early as possible and not propound discovery requests for such discovery that has been identified as unreasonably cumulative, duplicative, or obtainable from more convenient, less burdensome, or less expensive sources absent a showing of good cause.

    a. Requesting parties should be prepared to articulate the unique importance and benefit of discovery of non-U.S. sources as part of their Rule 26(f)(2) obligations.

    b. Requesting parties should consider responding party representations regarding discovery of non-U.S. sources that they believe are unreasonably cumulative, duplicative, or can be obtained from more convenient, less burdensome, or

less expensive sources and consider either limiting discovery sought to unique discovery from more convenient, less burdensome, and less expensive sources or articulate their good cause for seeking foreign discovery as part of their Rule 26(f)(3) discovery plan obligations.

c. Requesting parties should propound requests for non-U.S. discovery with reasonable particularity and in consideration of the inherent challenges of privacy and data protection compliance inherent in cross-border discovery as part of their Rule 34(b) and Rule 26(g) obligations.

d. As part of their Rule 26(b)(1) proportionality analysis, courts should take opportunities to proactively limit discovery of non-U.S. sources that have been identified and substantiated as unduly burdensome, unreasonably cumulative, duplicative, or obtainable from more convenient, less burdensome, or less expensive sources.

Practice Point 2: Parties should put in place, and courts should encourage, practices that promote compliance with data protection, labor, and confidentiality laws while also reducing the burden and expense of cross-border discovery, such as the following:

1. Discovery requests and responses limited in scope to what is relevant and proportional, particularly when addressing non-U.S. data sources

2. Protective orders and/or party stipulations and/or cost allocations pursuant to Rule 26(c) that include provisions recognizing compliance obligations for parties regarding non-U.S. data protection laws, potentially including:

   a. establishment of a defined classification for protected information[212]

   b. redactions of nonrelevant and/or unnecessary personal information

   c. security measures sufficient to comply with privacy and data protection laws and regulations, including breach notification requirements

   d. recognition of non-U.S. legal privilege claims subject to challenge and allowing for related redactions

   e. use limitations and attestation and certification requirements for any/all parties and non-parties accessing discovery

   f. detailed disposition and disposition certification requirements at close of case to ensure destruction of protected information

3. Scheduling orders that provide for phased or tiered discovery that prioritizes data sources without data protection challenges and allows sufficient time to implement

---

[212] *See International Litigation Principles*, *supra* note 2, at 39–58.

data protection safeguards

4. If utilized on a given case, ESI protocols that produce due respect for non-U.S. data protection requirements, such as data minimization

Practice Point 3: As they should with any argument resisting discovery on Rule 26(b)(1) grounds, parties making proportionality arguments based on the effects of compliance with non-U.S. data protection laws should support those arguments with specific detail about the expected burden or other disproportionate effects. This should include as much detailed accounting of potential costs and burden—monetary and otherwise—of the proposed discovery as is possible at the time. Parties facing discovery may choose to highlight costs related to compliance with data protection obligations, including time and costs to conduct data privacy law assessments, to confer and negotiate with data protection authorities, to conduct labor law assessments, and to negotiate with employee Works Councils. Parties may also highlight heightened costs associated with international eDiscovery data processing and hosting, costs for data privacy and labor law document review and redactions, and potentially for the application of pseudonymization or anonymization technologies. Such arguments may be aided by, for instance, published articles or commentary or case-specific statements provided by non-U.S. legal experts.

Practice Point 4: U.S. courts should appropriately consider the effect of a party's compliance with non-U.S. data protection laws as part of the case-specific proportionality analysis in determining the appropriate scope of discovery. Within such analysis, courts and parties should consider nonmonetary factors, including the data privacy interests of data subjects weighed against the importance of the issues as stake, how the parties' access to information is impacted by limitations caused by data protection laws, reputational risk that may result for violating non-U.S. data protection laws, and the risks of civil and criminal enforcement faced by producing parties.

Practice Point 5: Parties should consider avoiding a comity question by agreeing to the use of the Hague Evidence Convention, Chapter II, which provides a means for facilitating discovery by diplomatic officers, consular agents, and commissioners. In particular, Article 17 permits a duly appointed commissioner to "take evidence in the territory of a Contracting State in aid of proceedings commenced in the courts of another Contracting State," provided that a competent authority in the state where evidence will be taken gives permission, and that the commissioner complies with the authority's conditions. If parties to the U.S. litigation agree to this approach, non-U.S. data protection law concerns are minimized, assuming that data minimization occurs prior to transferring the information to the U.S., and the *Aérospatiale* comity analysis is not necessary.

Practice Point 6: Courts may minimize analytic and doctrinal problems relating to overlap of proportionality and comity factors by carefully addressing the distinct proportionality and comity analyses in order (see flowchart above). The proportionality analysis in Step 1 determines whether the requested information is discoverable, based on the articulated cost and noncost factors relating to the parties and litigation. The *Aérospatiale* comity analysis only comes into play after a court determines that the requested information is discoverable. In that comity analysis, the relevant factors to be considered also include the respective interests of the sovereign jurisdictions involved.