The Sedona Conference Journal®

Volume 25 ❖ 2024 ❖ Number Two

Articles

The Sedona Conference®

Antitrust Law, Complex Litigation, Intellectual Property Rights, and Data Security and Privacy Law

The Sedona Conference Journal®

Volume 25

■

2024

Number 2

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual or semi-annual basis, containing selections from the preceding year's conferences and Working Group efforts. A PDF copy of The Journal is available on a complimentary basis and can be downloaded from the Publications page on The Sedona Conference website: www.thesedonaconference.org. Check our website for further information about our conferences, Working Groups, and publications.

Comments (strongly encouraged) and requests to reproduce all or portions of this issue should be directed to:
The Sedona Conference,
301 East Bethany Home Road, Suite C-297, Phoenix, AZ 85012 or
info@sedonaconference.org or call 1-602-258-4910.

The Sedona Conference Journal® cover designed by MargoBDesignLLC at www.margobdesign.com.

Cite items in this volume to "25 Sedona Conf. J. _____ (2024)."

Publisher's Note

Welcome to Volume 25, Number 2, of *The Sedona Conference Journal* (ISSN 1530-4981), published by The Sedona Conference (TSC), a nonpartisan and nonprofit 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of complex civil litigation, intellectual property rights, international data transfers, data security and privacy law, and artificial intelligence. The mission of TSC is to move the law forward in a reasoned and just way through the creation and publication of nonpartisan consensus commentaries and advanced legal education for the bench and bar.

TSC employs three main strategies to achieve its mission. First, it conducts limited-attendance conferences of the nation's leading jurists, lawyers, academics, and experts to examine cutting-edge issues of law and policy. Second, Working Groups in TSC's Working Group Series pursue in-depth study of these legal issues and develop consensus-based nonpartisan commentaries of immediate and practical benefit to the bench and bar. Finally, TSC disseminates the learning developed in the conferences and by the Working Groups through accredited continuing legal education programs under The Sedona Conference Institute banner, various International Programmes on global legal issues, and webinars on a variety of topics. *The Sedona Conference Journal* supports all these activities.

Volume 25, Number 2, of the *Journal* contains two nonpartisan consensus commentaries from The Sedona Conference Working Group 11 on Data Security and Privacy Liability, one nonpartisan consensus commentary from Working Group 6 on International Electronic Information Management, Discovery, and Disclosure, and one nonpartisan consensus commentary from Working Group 10 on Patent Litigation Best Practices.

I would like to thank the editors of the Working Group commentaries published in this volume of the *Journal.* For more information about The Sedona Conference and its activities, please visit our website at www.thesedonaconference.org

Kenneth J. Withers
Executive Director
The Sedona Conference
December 2024

The Sedona Conference gratefully acknowledges the contributions of its Working Group Series annual sponsors (www.thesedonaconference.org/sponsors), event sponsors, members, and participants whose volunteer efforts and financial support make participation in The Sedona Conference and its activities a thought-provoking and inspiring experience.

Journal Editorial Board

The Sedona Conference Advisory Board

The Hon. Jerome B. Abrams (ret.), JAMS, Minneapolis, MN

The Hon. Hildy Bowbeer (ret.), St. Paul, MN

Kevin F. Brady, Esq., 3M, Avondale, PA

The Hon. Mitchell D. Dembin (ret.), San Diego, CA

The Hon. John Facciola (ret.), Washington, DC

The Hon. James L. Gale (ret.), Greensboro, NC

Prof. Steven S. Gensler, University of Oklahoma College of Law, Norman, OK

Ronald J. Hedges, Esq., Ronald J. Hedges LLC, Hackensack, NJ

The Hon. Paul R. Michel (ret.), Alexandria, VA

The Hon. Kristen L. Mix (ret.), JAG, Denver, CO

The Hon. Nan R. Nolan (ret.), Redgrave LLP, Chicago, IL

The Hon. Kathleen McDonald O'Malley (ret.), Sullivan & Cromwell LLP, Washington, DC

The Hon. Andrew J. Peck (ret.), DLA Piper, New York, NY

Jonathan M. Redgrave, Esq., Redgrave LLP, Washington, DC

The Hon. James M. Rosenbaum (ret.), JAMS, Minneapolis, MN

The Hon. Shira A. Scheindlin (ret.), Boies Schiller Flexner LLP, New York, NY

Daniel R. Shulman, Esq., Shulman Buske Reams PLLC, Minneapolis, MN

The Hon. Tom I. Vanaskie (ret.), Stevens & Lee, Scranton, PA

The Hon. Ira B. Warshawsky (ret.), Meyer, Suozzi, English & Klein, P.C., Garden City, NY

Judicial Advisory Board

The Hon. Michael M. Baylson, Senior U.S. District Judge, Eastern District of Pennsylvania

The Hon. Laurel Beeler, U.S. Magistrate Judge, Northern District of California

The Hon. Cathy A. Bencivengo, U.S. District Judge, Southern District of California

The Hon. Cathy Bissoon, U.S. District Judge, Western District of Pennsylvania

The Hon. Ron Clark, Senior U.S. District Judge, Eastern District of Texas

The Hon. Joy Flowers Conti, Senior U.S. District Judge, Western District of Pennsylvania

The Hon. George C. Hanks, Jr., U.S. District Judge, Southern District of Texas

The Hon. Susan Illston, Senior U.S. District Judge, Northern District of California

The Hon. Kent A. Jordan, U.S. Appellate Judge, Third Circuit

The Hon. Barbara M.G. Lynn, Senior U.S. District Judge, Northern District of Texas

The Hon. Katharine H. Parker, U.S. Magistrate Judge, Southern District of New York

The Hon. Anthony E. Porcelli, U.S. Magistrate Judge, Middle District of Florida

The Hon. Xavier Rodriguez, U.S. District Judge, Western District of Texas

The Hon. Lee H. Rosenthal, U.S. District Judge, Southern District of Texas

The Hon. Elizabeth A. Stafford, U.S. Magistrate Judge, Eastern District of Michigan

The Hon. Gail J. Standish, U.S. Magistrate Judge, Central District of California

The Hon. Leda Dunn Wettre, U.S. Magistrate Judge, District of New Jersey

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

COMMENTARY ON PROPOSED MODEL DATA BREACH NOTIFICATION LAW

A Project of the Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

Author:

The Sedona Conference

Editor-in-Chief:

Matthew Meade

Contributing Editors:

Kamal Ghali
Amy Keller
Ryan G. Kriger
Ruth Promislow
David Sella-Villa
Martin T. Tully
Hon. Thomas I. Vanaskie (ret.)
W. Lawrence Wescott

Steering Committee Liaison

Alfred J. Saikali

Staff Editors:

David Lumia
Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 11. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of

the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

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.

This publication may be cited as follows:

> The Sedona Conference, *Commentary on Proposed Model Data Breach Notification Law*, 25 SEDONA CONF. J. 543 (forthcoming 2024).

PREFACE

Welcome to the August 2024 final version of The Sedona Conference's *Commentary on Proposed Model Data Breach Notification Law ("Commentary")*, a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). 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 WG11 is to identify and comment on trends in data security and privacy law, in an effort to help organizations prepare for and respond to data breaches, and to assist attorneys and judicial officers in resolving questions of legal liability and damages.

The Sedona Conference acknowledges Editor-in-Chief Matt Meade for his leadership and commitment to the project. We also thank contributing editors Kamal Ghali, Amy Keller, Ryan Kriger, Ruth Promislow, David Sella-Villa, Martin Tully, Judge Tom Vanaskie, and Larry Wescott for their efforts. We also thank Al Saikali for his contributions as Steering Committee liaison to the project. We thank Daryl Osuch, Emma Lombard, and Julia Veeser for their contributions.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG11 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 WG11 meetings where drafts of this *Commentary* were the subject of the dialogue. The publication was also subject to a period of public comment. On behalf of The

Sedona Conference, I thank both the membership and the public for all of their contributions to the *Commentary*.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, 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
Executive Director
The Sedona Conference
August 2024

TABLE OF CONTENTS

I. INTRODUCTION

In 2002, California became the first U.S. state to adopt a data breach notification law, which became effective on July 1, 2003.[1] Since then, a patchwork system of inconsistent data breach notification laws was gradually enacted in other states, with all fifty U.S. states now having enacted some form of notification law. Generally speaking, data breach notification laws require those affected by a data breach (or unauthorized access to data) to notify individuals, customers, and other parties about the breach, as well as take specific steps to remedy the situation based on directives of the state legislature.

Data breach notification laws are typically viewed as having two main goals. The first is to timely notify individuals whose data was involved in a breach in order to give them the chance to mitigate damage and risks caused by the data breach. The second is to increase accountability of organizations and encourage them to strengthen data security. But the laws, as written, do not necessarily accomplish those goals for two chief reasons.

First is the issue of uniformity. There are important differences among the measures adopted by different states. Differences in data breach notification laws include varying definitions of personally identifiable information ("PII"), with corresponding variations of notice obligations to impacted individuals, law enforcement, and consumer credit agencies. Another difference is varying penalties for noncompliance. This lack of uniformity makes it challenging for breached entities to understand their obligations and makes it more complicated and expensive to comply with the law. This is a particular issue for smaller organizations that do not have the resources to retain external privacy counsel.

---

1. SB 1386, CAL. CIV. CODE § 1798.82 and 1798.29.

Second, most notification letters do little to help consumers. When a data breach occurs, individuals whose data was involved in the breach will likely receive a standardized letter that vaguely explains what happened, why they should not be panicked, and a general discussion of the type of data that was involved in the breach. Typically, the notification does little to inform consumers of how to protect themselves through certain mitigating measures—such as freezing their credit or enrolling in a credit monitoring service. The vague nature of the notices, combined with the fact that consumers are receiving more and more notices specifically telling them not to worry, can lead to fatigue and, eventually, data security apathy.

This *Commentary* is intended to assist federal and state lawmakers to update or enact data breach notification laws that: (i) enable individuals to protect themselves against the risk of data breaches; and (ii) provide concise, clear, and consistent direction to PII Controllers (defined below) responding to data security incidents. This *Commentary* was prepared over the course of several years by a cross-section of experienced privacy lawyers, technology experts, and regulatory authorities who seek to reduce conflict between and lack of clarity within the various state data breach notification laws.

The *Commentary* addresses the aforementioned two chief problems with present data beach notification statutes and suggests eight areas where the current iterations of state data breach notification laws can be improved by greater uniformity and clarity: (1) definition of Security Breach; (2) definition of PII; (3) definition of risk of harm; (4) encryption, de-identification, and similar technologies; (5) method and form of notification; (6) timeline for notification; (7) credit monitoring; and (8) notifying law enforcement and regulatory authorities.

For ease of reference, we have compiled the proposed model language for each of the eight areas identified above in their

entirety in Section IV of this *Commentary*. Because of the interplay among them, it is essential to the formulation and subsequent use of this proposed language that the eight sections be considered as a whole. While there are other significant topics addressed in state data breach notification laws that are not covered within the eight areas, e.g., private right of action, notification to consumer reporting agencies, definitions of records, covered entities, substitute notice, law enforcement delay, form of regulator notice, etc., the *Commentary* focuses principally on these eight areas because, based upon collective experience, these areas would benefit the most from the uniformity and clarity of a Model Data Breach Notification Law.

This *Commentary* is intended to inform policy decisions at the federal or state levels as data breach statutes evolve. Even if a legislature declines to adopt all of the recommendations made herein, it may benefit from the analysis as to specific elements of such a law.

II. BACKGROUND

Security breach notification laws can impose obligations on any PII Controller,[2] regardless of its size, sophistication, or industry. Similarly, all organizations are vulnerable to security breaches, regardless of how mindful they are of data security. PII Controllers frequently experience security incidents that may give rise to breach notice obligations.[3]

The number of data breaches and data security incidents continues to rise; however, requiring that *all* security incidents be reported, and notice sent, would not be good policy. This would lead to notice fatigue among notice recipients, who would likely start ignoring notices, even ones of critical importance. Professor Rui Chen of Iowa State University has described a trend that he calls "data breach fatigue," where people do not appear to be concerned about their data security, despite recent major data breaches.[4] Professor Chen observed, "[w]hen an incident happens, when a data breach incident goes to the media, people read that news and they start to lose interest . . . .

---

2. "PII Controller" means any entity, including a government entity, that collects, receives, maintains, possesses, controls, or has custody of PII. *See* Section IV.A.

3. For purposes of this document, a "security incident" refers to an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. *Security incident*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, COMPUTER SECURITY RESOURCE CENTER, https://csrc.nist.gov/glossary/term/security_incident (last visited Aug. 2, 2024). All security breaches begin with a security incident, but not all security incidents turn out to be security breaches.

4. Grayson Schmidt, *Expert Warns of the Risks Posed by Data Breach Fatigue*, AMES TRIBUNE (Jan. 31, 2018), https://www.govtech.com/security/Expert-Warns-of-the-Risks-Posed-by-Data-Breach-Fatigue.html.

They take it as a new normal in today's society."[5] Unfortunately, as a result, individuals may not take steps to protect themselves from further loss and injuries or may not understand what steps they may take to do so.[6] This potential notice fatigue may mean that consumers will not engage in routine, common-sense measures to mitigate their losses—such as taking the time to freeze their credit, monitor their credit reports (or purchase credit monitoring services to do that for them), or routinely monitor already-open credit files.

Further, requiring overly broad notice may impose an unnecessary burden on the business community. As discussed in more detail in Section IV, a Model Data Breach Notification Law should be tailored to require that only certain incidents be considered reportable security breaches.

The analysis of whether a given security incident triggers a notice obligation can be time-consuming and costly. If the media affected includes email, file systems, backup tapes, or paper records, search algorithms might not suffice, and entities seeking to ascertain if a notice obligation exists might be required to pore over terabytes of data by hand. Often, forensic investigators must be retained by the entity to determine exactly what happened and, working with counsel, to determine whether an incident triggers a notice obligation.[7] In addition to expense,

---

5. *Id.*

6. This *Commentary* does not suggest that the burden should be on consumers to take affirmative steps to mitigate risk after data breaches; rather, it acknowledges the current legal and regulatory landscape requires that consumers take affirmative acts to protect themselves—*e.g.*, enrolling in credit monitoring or electing to freeze their credit—as protective measures are not automatically in place for consumers.

7. It is worth noting that all entities should employ data minimization techniques and data mapping to have a wholesome understanding of the data they maintain, as well as comply with newer privacy laws.

these activities take time, during which individuals who may be vulnerable to fraud and identity theft by reason of the security incident are not made aware of their exposure. These activities are also expensive for PII Controllers and their insurers. Thus, a Model Data Breach Notification Law should be drafted to make it as clear as possible what constitutes a notification-triggering security incident requiring such investigation and should be drafted with the complexities and costs of compliance in mind.

While a Model Data Breach Notification Law must be narrowly tailored to be manageable by PII Controllers, it must remain broad enough to ensure that individuals are notified of a security incident when circumstances warrant notification—such as when such incidents put them at increased risk of identity theft, or when they might experience reputational harm, among other things. Any consideration of what should or should not be included in such a law must be guided by the fundamental need to inform individuals of such a security event so that they may take steps to mitigate against further loss.

It is critical that a Model Data Breach Notification Law should be drafted with these principles in mind.

III. ANALYSIS AND DISCUSSION OF CURRENT STATE DATA BREACH NOTIFICATION LAWS

Set forth below is an analysis of areas of current state data breach notification laws that this *Commentary* seeks to address.

A. Is PII Involved in the Incident?

The first step in determining whether an entity would need to send notice pursuant to the proposed model statute is determining whether PII was involved in the incident. PII is information that, when used alone or with other data, can identify an individual. An entity that does not collect PII need not worry about having to provide notice to individuals of data security incidents, and entities that do collect PII can take steps to segment such data or focus their data protection efforts on such data in order to minimize their risk of suffering a notice-triggering incident.

B. If the Incident Involves PII, Is It a Security Breach?

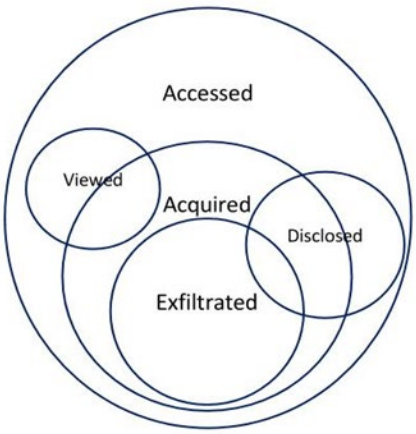
1. Inconsistencies in Current State Law on What Should Constitute a Notifiable Data Breach

After determining that PII was affected by a security incident, the next step in determining whether notification is required is to assess whether the incident constitutes a data breach.[8] If PII was involved, the next question is whether the unauthorized user interacted with the data in a manner that

8. *See* Fero v. Excellus Health Plan, Inc., 304 F. Supp. 3d. 333, 339 (W.D.N.Y. 2018) ("plaintiffs had standing to bring data breach claims when the breached database contained personal information such as 'names, dates of birth, marital statuses, genders, occupations, employers, Social Security Numbers, and Driver's license numbers."), *citing* Whalen v. Michaels Stores, Inc., 689 Fed. App'x 89, 91 (2d. Cir. 2017). Virtually every state data breach notification law covers personal information.

may necessitate notice. The terms most often used by state notification statutes in defining what must have happened to the data in question for the statutes to apply include *accessed*, *viewed*, *disclosed*, *acquired*, and *exfiltrated*.

These different terms are subject to interpretation and debate—the Venn diagram below provides one such interpretation:



Access is considered the broadest definition. For example, in the context of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, et. seq., a defendant was found to have "accessed" America Online's computers by sending email through them: "For purposes of the CFAA, when someone sends an email message from his or her own computer, and the message then is transmitted through a number of other computers until it reaches its destination, the sender is making use of all of those computers and is therefore 'accessing' them."[9]

A minority of states use the "access" approach.[10] "Acquisition" is considered a narrower definition and has been adopted

9. Am. Online, Inc. v. Nat'l Health Care Discount, Inc., 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000).

10. *See, e.g.*, FLA. STAT. ANN. § 501.171(1)(a) ("'Breach of security' or 'breach' means unauthorized access of data in electronic form containing

by the vast majority of states.[11] However, the trend may be beginning to move in the other direction. New York recently moved from acquisition to access.[12]

---

personal information."); N.J. STAT. ANN. § 56:8-163(a) ("Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person."); CONN. GEN. STAT. ANN. § 36a-701b(a) ("'breach of security' means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data, containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable."); R.I. GEN. LAWS ANN. § 11-49.3-3(a)(1) ("'Breach of the security of the system' means unauthorized access or acquisition of unencrypted, computerized data information that compromises the security, confidentiality, or integrity of personal information maintained by the municipal agency, state agency, or person.); P.R. LAWS ANN. tit. 10 § 4051(c) ("Violation of the security system. — Means any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised . . . .").

11. *See, e.g.*, COLO. REV. STAT. ANN. § 6-1-716(h) ("'Security breach' means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity."); MINN. STAT. ANN. § 325E.61(1)(d) ("'breach of the security of the system' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."); UTAH CODE ANN. § 13-44-102(1)(a) ("'Breach of system security' means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.").

12. *See* N.Y. GEN. BUS. LAW § 899-aa(c) ("'Breach of the security of the system' shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that comprises the security, confidentiality, or integrity of private information maintained by a business.").

Some states have recognized that it is difficult to determine absolutely that access took place due to insufficient logging or log retention, sophisticated attackers, or intervening circumstances. These states require that a PII Controller report a breach if it has a *reasonable belief* of access without providing any examples of what constitutes a reasonable belief.[13]

Due to the potential difficulty in distinguishing whether a threat actor has acquired data because of the sophistication of the threat actor or insufficient logging by the breached entity, the Drafting Team believes a broad definition of "Security Breach" is appropriate. The *Commentary*'s proposed Model Date Breach Notification Law hinges the definition on unauthorized access to PII, rather than unauthorized acquisition, disclosure, or theft, for example. This approach simplifies the analysis necessary to determine whether notice should be provided and can help avoid incentivizing businesses to collect *less* logging information in order to be able to claim an inability to establish acquisition.

While a broader definition of "Security Breach" could include access to data or a circumstance that would lead a

13. *See, e.g.*, ALASKA STAT. § 45.48.090(1) ("'breach of the security' means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector . . . ."). The concept of reasonable belief is also sometimes applied to a risk of harm analysis, though for purposes of this analysis we are limiting its use to the access or acquisition of data. *See* KY. REV. STAT. ANN. § 365.732(1)(a) ("'Breach of the security of the system' means unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky.").

reasonable PII Controller to believe that an unauthorized access to unencrypted data has occurred—regardless of whether that access compromises the security, confidentiality, or integrity of an individual's PII maintained by that PII Controller—this definition would be so broad that it would include certain security incidents that would have very little likelihood of harm to individuals whose PII was accessed. Excluding those incidents would have the benefit of encouraging PII Controllers to adopt best practices. One such exclusion would be for unauthorized access to encrypted or sufficiently de-identified data.[14] Where the accessed data is encrypted with sufficient security measures or de-identified in a way that prevents a threat actor from accessing the data, it should be unusable by bad actors. For this reason, access to encrypted or de-identified data should not be considered a security incident potentially worthy of requiring notice, unless the bad actor also possesses the encryption key or is otherwise likely able to reidentify the data.[15] Additionally,

14. Many states include the issue of encryption in the definition of PII instead of the definition of Security Breach. We believe it is more appropriately addressed in another section of the proposed model statute. This is because if a business collects social security numbers, for example, it may be encrypted at rest, but at some point it may be available in an unencrypted form. If the data is acquired while unencrypted, it is a breach. If PII is defined as "unencrypted data," then whether a business holds PII can change based on the state or use of the data.

15. *See, e.g.*, TEX. BUS. & COM. CODE § 521.053(a) ("In this section, 'breach of system security' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data."); CAL. CIV. CODE § 1798.29(a) ("Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by

there are several different encryption techniques and algorithms, some of which are no longer effective. Thus, encryption should be separately defined to mean, "a technology for securing computerized data in such a manner that it is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key that is not accessible by unauthorized persons." While an exclusion for encrypted data could be built into the definition of "Security Breach" or the definition of "PII," the clearest way to create such an exclusion is by a separate statutory provision. (See further discussion of encryption, de-identification and related technologies in Section III.E.)

Another situation in which there is a low likelihood of injury to the individual(s) in question exists where data is accessed by someone without authorization, but the access was made in good faith by an internal employee, or an agent, for authorized business purposes. Thus, an exception from the definition of Security Breach should be made for this situation, as is already common in many data breach laws.[16]

---

an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable.").

16. *See* IOWA CODE § 715C.1(1) ("Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.").

2. Challenges Created by Current Laws

The use of the term "acquisition" as the means of data interaction for triggering a potential notice obligation is not only less consumer-friendly but also may create difficulties in the cloud computing context. Threat actors may still "access" information in cloud computing environments without "acquiring" it, leading to a significant risk of harm to the individuals whose data is housed in the cloud. State statutes that use the term "acquisition" without a corresponding "risk of harm" analysis (as discussed below) significantly disadvantage individuals whose data is impacted by a security incident. This can also lead to further confusion among PII Controllers, who will need to implement different notice thresholds in different states.

Finally, because security incidents are often very specific, and listing all possible variations of a "harmless" breach would be futile, it would be worthwhile to insert a "catch-all" provision for access to data that is unlikely to lead to harm (see Risk of Harm discussion, below). This determination, however, should be made by a data collector , as otherwise the incentive would be too great for a PII Controller to rationalize why any individual breach is unlikely to lead to harm.

C. The Type of PII Involved Determines Whether Notification Is Necessary

Currently, state data breach notice laws vary significantly in their definitions of what sorts of PII can trigger a notice obligation. Most states contain a laundry list of data elements that are amended from time to time in order to keep up with advances in technology. These lists can and do vary widely from state to state.

Further, the nature of data breaches has evolved to include an increased scope of PII. Previously, data breaches typically involved financial or other information that could be used to

commit identity theft. Now, threat actors are increasingly focused on acquiring a much broader scope of personal information, including private information, and then commoditizing that information for purposes beyond financial fraud. For these reasons, the *Commentary*'s two-tiered approach to defining PII means that harm beyond economic loss—such as bodily harm, psychological distress, damage to reputation or relationships, or loss of employment, business, or professional opportunities—may require notice.

1. Current State Data Breach Notification Laws

In the United States, there are varying definitions of PII among the states. Each state's data breach notification law specifies the particular information that is defined to be "personal," such that a compromise of that kind of information may amount to a reportable breach. The definition of PII in these state breach notification laws is therefore static. That is, there is no flexibility in the statute to interpret the definition of PII to include a category of information that is not expressly identified.

This static approach to defining PII does not account for the evolving cyber threat landscape, where new types of information associated with individuals are compromised, and which can cause the same or greater level of harm as the compromise of traditionally recognized categories of PII. For example, categories of personal information that are increasingly compromised include a data subject's contact list, geolocation data, and employment information. As more of our business and personal lives are conducted online, and as PII continues to be commoditized through behavioral and targeted advertising, the ability of threat actors to monetize increasing categories of personal information continues to expand. A static definition of PII fails to account for this evolving threat.

This threat to an expanding number of categories of personal information can also be attributed to the increasing digitization of records by businesses of all sizes and across all industries. This move toward a digital economy contributes to the expansion of information associated with individuals that is subject to compromise in a security incident.

Additionally, a static definition of PII does not account for new categories of personal information that may be at risk as technologies emerge, such as biometrics (which is included in the definition of PII in some state breach notification laws), behavioral modeling, and information captured by voice assistants or connected vehicles.

A static approach to defining PII requires legislative reform as new categories of PII are revealed to be at risk of giving rise to harm when subjected to unauthorized access.

2. Current Compliance Challenges

The practical problem that a PII Controller faces in the event of a security incident is the conflicting state regimes with which it must comply. What may constitute a reportable incident in one state is not necessarily so in another.

The fact that a state breach notification law has included a particular category of information in the definition of PII implies that a compromise of such data could give rise to harm. Likewise, the absence of a particular category of information from the specific list of PII in the state breach notification law suggests that a compromise of such information would not give rise to harm in that jurisdiction. For that reason, notice to impacted individuals involving that omitted category of information is not required. But data is not different depending on jurisdiction, and state-by-state definitions of PII have created more complications than benefits to governments, entities, and individuals. Based on those categories of information identified

in the definition of PII, a PII Controller may develop a data protection strategy that focuses on protecting listed categories of information. In this way, the state breach notification laws indirectly incentivize PII Controllers to implement reasonable safeguards for the categories of information included in the definition of PII. However, the varying and conflicting definitions of PII in the state breach notification laws create inconsistent incentives for organizations in developing their data protection strategy.

The following types of information associated with individuals have been included in various states' definitions of PII:

- Social Security number;
- motor vehicle operator's license number or non-driver identification card number;
- financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;
- account passwords or personal identification numbers or other access codes for a financial account;
- biometric information, including a fingerprint, retinal scan, and facial recognition data;
- genetic information;
- health information;
- health insurance policy number or health insurance identification number and any unique identifier used by a health insurer to identify an individual;
- login credentials, including a username or password; and
- passport number.

Specific examples of the discrepancies with respect to the definition of PII are as follows:

Biometric data is included in the definition of PII in several states, including Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Illinois, Iowa, Louisiana, Maryland, Michigan, Nebraska, New Mexico, North Carolina, South Carolina, South Dakota, Texas, Vermont, and Wisconsin,[17] but not in others such as Alabama, Indiana, Kansas, Massachusetts, and Nevada.[18]

Passport number is included in the definition of PII in states such as Alabama, Arizona, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Kentucky, Louisiana, Maryland, Michigan, North Carolina, and Vermont,[19] but not in

17. ARIZ. REV. STAT. § 44-7501(11); ARK. CODE. ANN. § 4-110-103(7); CAL. CIV. CODE ANN. § 1798.29(g); COLO. REV. STAT. ANN. § 6-1-716(g); CONN. GEN STAT. § 36a-701b(a); DEL. CODE. ANN. tit. 6 §12B-101(7); D.C. CODE ANN. § 22–3227.01(3); ILL. COMP. STAT. ANN. ch. 815 § 530/5(1)(F); IOWA CODE § 715C.1(11); LA. REV. STAT. § 51:3073(4)(a); MD. COM. LAW. CODE ANN. §14-3501(e); MICH. COMP. LAWS ANN. § 445.63(q); NEB. REV. STAT. § 87-802(5); N.M. STAT. ANN. § 57-12C-2(C); N.C. GEN. STAT. ANN. § 75-66(c); S.C. CODE ANN. § 30-2-30(1); S.D. CODIFIED LAWS § 22-40-19(4); TEX. BUS. COM. CODE § 521.002(a); VT. STAT. ANN. tit. 9 § 2430 (10); WIS. STAT. ANN. § 134.98(1)(b). On June 6, 2023, Florida Governor Ron DeSantis signed Senate Bill 262 to create the Florida Digital Bill of Rights which includes language to expand the definition of PII in Florida's breach notification law to include biometric data, effective July 1, 2024.

18. CODE OF ALA. § 8-38-2(6); FLA. STAT. ANN. § 501.171(1)(g); IND. CODE. ANN. § 24-4.9-2-10; KAN. STAT. ANN. § 50-7a01(g); MASS. GEN. LAWS ANN. ch. 93H, § 1(a); NEV. REV. STAT. ANN. § 603A.040(1).

19. CODE OF ALA. § 8-38-2(6); ARIZ. REV. STAT. § 44-7501(11); CAL. CIV. CODE ANN. § 1798.29(g); COLO. REV. STAT. ANN. § 6-1-716(1)(g); CONN. GEN STAT. § 36a-701b(a); DEL. CODE. ANN. tit. 6 § 12B-101(7); D.C. CODE ANN. § 22–3227.01(3); FLA. STAT. ANN. § 501.171(1)(g); KY. REV. STAT. ANN. § 365.720(4); LA. REV. STAT. § 51:3073(4)(a); MD. COM. LAW. CODE ANN. § 14-3501(e); N.C. GEN. STAT. ANN. § 75-66(c); VT. STAT. ANN. tit. 9 § 2430 (10); VA. CODE ANN. § 18.2-186.6(A).

others such as Arkansas, Indiana, Massachusetts, Minnesota, Nebraska, New Mexico, Nevada, and Rhode Island.[20]

A broad definition of PII serves to clarify the obligations on PII Controllers with respect to their obligations in protecting PII.

3. Guidance Regarding the Scope of PII

A potential criticism of a broad PII definition is that PII Controllers will not have advance notice of the specific types of PII that could trigger a notice obligation if accessed without authorization, and that PII Controllers may be penalized for failing to provide notice based on unauthorized access to data that they did not consider to be PII. However, the proposed definition, while broad, is clear and straightforward: it covers factual or subjective information about, pertaining to, or traceable to, an identifiable individual.

Guidance is provided on the scope of PII as follows:

- Information will pertain to, be traceable to, or be about an identifiable individual, even where the information does not itself identify that individual, where it is more likely than not that an individual could be identified through the use of that information, either alone or in combination with other information.
- Information can meet the definition of PII regardless of how it was accessed or acquired, including information voluntarily provided, or observed, derived, or inferred from nonconfidential source material.

20. *See id*; MINN. STAT. ANN. § 325E.61(1)(e); R.I. GEN. LAWS § 11-49.3-3(a)(8).

The following is an illustrative but nonexhaustive list of classes of PII (either by itself or in connection with other PII) to aid in current understanding and future analysis:

- Name (including full name);
- Government-issued numbers or other unique identifiers (social security numbers, passport numbers, motor vehicle operator's license numbers, state identification card numbers, etc.);
- Dates pertaining to an individual (birth date, wedding date, graduation date, death date, military enlistment or discharge date, etc.);
- Financial account numbers—real or virtual (any bank account numbers, credit card numbers, investment or retirement account numbers, virtual currency account numbers, etc.);
- Any login credentials (email address, username, password or other access code such as a personal identification number ("pin" or "pin number"), or security question or password recovery answers);
- Biometric data (more specifically, an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity);
- Insurance information (identification numbers, insurance policy numbers, or any other unique identifying number);
- Health information (health history, information about illnesses, information or observations about a patient, etc.);

- Employee personnel files or similar evaluations or personal commentary (subjective or objective employee performance metrics, any kind of personal analysis, goals that might be about an identifiable individual, etc.);
- Physical asset information that consistently links an item to an individual (Media Access Control (MAC) address, Internet Protocol (IP) address, car license plate number, home address);
- Geolocation data (such as data used on ride-sharing apps, shopping or discount apps, augmented-reality apps or games);
- Customer loyalty or affinity account numbers;
- Physical asset or software usage data (browser history, cookies, software tokens, usage metadata, etc.); or
- Any other unique, number-based code or characteristic that is about an identifiable individual (phone number, an organizational anonymized code for an individual, etc.).

4. International Trends Regarding PII

Smart phones and devices—and, therefore, applications that collect, maintain, and control PII—are used by individuals domestically and internationally. Accordingly, there is value in moving toward a definition of PII that more closely aligns with the international approach. Increasingly, PII Controllers conduct business in multiple jurisdictions and are required to comply with varying, conflicting regulatory regimes. Incentivizing PII Controllers to take privacy seriously and to incorporate privacy by design is supported by moving toward the broader approach to defining PII globally.

The General Data Protection Regulation (GDPR), a law that imposes obligations and regulations on entities that target or collect data related to individuals in the European Union, uses a broad definition of PII. "Personal data" is defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[21]

Likewise, the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) uses a broad definition of PII. Under PIPEDA, personal information is defined as "information about an identifiable individual."[22] In guidelines issued by the Office of the Privacy Commissioner (which oversees the administration of PIPEDA), PII is further explained to be "any factual or subjective information, recorded or not, about an identifiable individual," and examples of PII are provided.[23]

For the reasons discussed herein, the *Commentary* proposes a two-tiered definition of PII that will provide clarity to PII

---

21. 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), art. 4 (1), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents.

22. Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5, § 2(1).

23. *PIPEDA requirements in brief*, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/ (last visited Aug. 2, 2024).

Controllers so that determinations of notification obligations can be more easily made.

Category I PII includes, among other things as listed in the draft of the Model Law, Social Security numbers, driver's license numbers, and sensitive health information; financial information; and account and login credentials. Any PII Controller that has experienced a Security Breach involving Category I PII may seek to determine as to any PII Subject associated with the PII in question whether the Security Breach as to that associated PII is unlikely to have caused and is unlikely to cause Harm to that PII Subject.

Category II PII includes but is not limited to date of birth; maiden name of the individual's mother; digitized or other electronic signature; insurance information (identification numbers, insurance policy numbers, or any other unique identifying number); health information that is not sensitive diagnosis information (health history, information about illnesses, information or observations about a patient, etc.) Any PII Controller that has experienced a Security Breach of Category II PII shall determine as to each PII Subject associated with the PII in question whether the Security Breach as to that associated PII has likely caused or is likely to cause Harm to that PII Subject.

D. What Role Should Risk of Harm Analysis Play in Data Breach Notification?

Because the nature of data breaches has evolved to include an increased scope of PII, the scope of harm has likewise evolved. Accordingly, the next step in determining whether notification of a security incident is required involves performing a "risk of harm" analysis. Put in the simplest of terms: if an individual is likely not to experience harm as a result of a Security Breach, then providing notice to that individual is

unnecessary.[24] The vast majority of state data breach notification laws require some analysis by the impacted PII Controller of the risk of harm to the individual associated with the PII in question by reason of the event in question before a notification requirement is triggered. The standard for determining whether a sufficient risk of harm exists to require notification varies across those states, however, and uniformity is necessary to eliminate confusion.

1. The Variation in Risk-of-Harm Standards and Definitions Is Problematic

For most states, the statutory formulations require *some* degree of likelihood of *some* sort of harm to the individual associated with the PII in question in order to trigger a notice obligation to the individual affected. The statutory formulations vary widely, however, in regard to *what* sort of harm and to *what* degree of likelihood that harm must exist for notice to be required. For example, in New Jersey, notification is not required if the business or public entity establishes that misuse of the information is not reasonably possible.[25] In North Carolina, notification is not required if a breach does not result in illegal use of PII, is not reasonably likely to result in illegal use, or there is no material risk of harm to a consumer.[26] In Massachusetts,

24. This statutory "risk of harm" analysis for breach notification is related to but very distinct from the question of whether "concrete, particularized harm" or "intangible" injury exists—including the "risk" of injury—that is central to whether plaintiffs have standing to sue over a data breach and whether their claims are viable. The "risk of harm" analysis for statutory data breach notification purposes presents different concerns from the "injury" requirement for Article III standing. Accordingly, this *Commentary* refers only to "risk of harm" in statutory construction and is not intended to provide any analysis concerning venue or jurisdiction in litigation.

25. N.J. STAT. ANN. § 56:8-163(a).

26. N.C. GEN. STAT. § 75-61(14).

notification is required where the breach creates a "substantial risk of identity theft or fraud against a resident of the Commonwealth," or when the person or agency knows or has reason to know that the PII of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose.[27] In Indiana, notification is required "if the database owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity theft, or fraud affecting the Indiana resident."[28] Under other frameworks, there is a presumption of harm (and thus a requirement to give notice) unless it is "reasonable" to conclude otherwise.[29]

The current statutory formulations of the risk-of-harm standard are problematic for two reasons. First, the differences between the formulations create the distinct possibility of identical facts triggering a notice obligation in one jurisdiction but not in another. Second, the vagueness of those formulations arguably denies PII Controllers fair notice of what the formulations require, and that vagueness at a minimum creates an undesirable range of differing, but reasonable, interpretations of those requirements. For example, the use of subjective terms like "low," "high," "significant," "material," "reasonably," and "substantial" to define how likely the harm in question must be for a notice obligation to exist leaves the decision of whether a notice obligation has been triggered very much in the eye of the beholder. And this problem is exacerbated by those statutory formulations that, rather than following the example of states

27. *See* IOWA CODE § 715C.1(1).

28. IND. CODE ANN. § 24-4.9-3-1(a).

29. Looking to Europe, the GDPR requires personal notifications when the personal data breach is likely to result in a "high risk to the rights and freedoms of natural persons," unless certain conditions are met. *See generally* General Data Protection Regulation, *supra* note 21, article 35.

like Indiana (which, as noted, defines the relevant "harm" as "identity deception, identity theft, or fraud"), provide no definition at all of what constitutes "harm" for purposes of the statute, and thus leave that core issue wholly open to interpretation and subjective judgment. The likely result? Breached entities will likely conclude that no risk of harm resulted at all.

A requirement that the acquisition/access is "reasonably likely to cause injury or identity theft or fraud" leaves the determination solely in the hands of the data collector or owner. Some PII Controllers may underestimate or misunderstand the potential risk of harm and inadvertently default to finding that the likelihood of injury is low and therefore not be incentivized to provide notice to individuals. Others may be incentivized to find that no harm exists given the cost of sending notice. Under other frameworks, there is a presumption of harm (and thus a requirement to give notice) unless reasonable to conclude otherwise. In tacit recognition of the interpretive problems created by the current statutory formulations of the risk-of-harm standard, some state statutes inject the relevant regulator into the process by which PII Controllers apply the risk-of-harm standard. Vermont, for example, has a "negative option" harm trigger stating that if a data PII Controller believes misuse of personal information is not reasonably possible, and it informs the Attorney General, it need not notify potentially affected persons.[30] Florida requires that the risk-of-harm analysis be conducted in consultation with relevant federal, state, or local law enforcement agencies.[31] Alaska similarly requires the giving of notice to the state Attorney General as a condition of determining that no reasonable likelihood of harm exists.[32] Presumably, statutory

30. VT. STAT. ANN. tit. 9 § 2435(d).

31. FLA. STAT. ANN. § 501.171(4)(c).

32. ALASKA STAT. ANN. § 45.48.101(c).

provisions like these are premised on a concern that because the statute's risk-of-harm standard is vague and subjective, and if the statute leaves the risk-of-harm determination solely in the hands of the PII Controller, breach notification that the relevant regulator believes should be given will not be given. Whatever the merit may be of such statutory provisions and the policy concerns on which they are presumably premised, the *Commentary* views these "run it by the regulator" provisions as corroboratory of the highly problematic vagueness and subjectivity built into the current statutory formulations of the risk-of-harm standard.

2. Considerations to Address Issues Created by Various Risk-of-Harm Standards

The statutory framework for the Health Insurance Portability and Accountability Act ("HIPAA") provides a helpful analysis in determining when notification of a Security Breach is necessary. Under that statute, the "acquisition, access, use, or disclosure of protected health information in a manner not permitted" under the statute is presumed to be a breach "unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment" constituting four factors.[33] Following those factors provides guidance and a framework for assessing risk of harm in other data contexts.

a. The Nature and Extent of the Information Involved

Consider the nature and extent of the PII involved. Is it sensitive information? Is it financial? Could it be used for extortion

33. CFR § 164.402(2).

or to hurt someone's reputation? What type of information was inappropriately disclosed or used? Would the unauthorized access, unavailability, or modification of the PII likely harm the data subject? (See discussion of what constitutes PII in Section IV.A.)[34]

b. The Recipient of the PII

Consider the unauthorized person who accessed the PII. This analysis is different from any analysis performed to determine if a Security Breach has occurred. Is the recipient a criminal actor? Also consider whether this person has legal obligations to protect the information—for example, is the person or entity required to comply with confidentiality or nondisclosure obligations or applicable privacy laws? If so, there may be a lower probability that the PII has been compromised. Also consider if the unauthorized person has the ability to reidentify or decrypt the information.

c. Whether the PII Was Actually Acquired, Used, or Viewed

In other instances, it may be possible to determine that the PII accessed as a result of the security incident has not, in fact, been viewed or used in a manner that likely caused or is likely to cause the requisite harm.[35] For example, this would be the

34. As discussed in the Proposed Model Data Breach Notification Law, at IV.D., if there is reason to believe that a prior risk of harm analysis has changed (e.g., the PII Controller determined that there was no risk of harm, but the information was later found on the dark web), the PII Controller should reexamine the analysis and provide notice if necessary.

35. Some security incidents may fall into another type of safe harbor because the PII was encrypted, de-identified, anonymized, or otherwise rendered inaccessible, and therefore not reasonably likely to ever be used or viewed. But this consideration, while important, goes to whether or not a Security Breach even occurred.

case if a laptop containing PII is stolen but soon after tracked to a pawnshop, where it is determined that the laptop was never actually accessed or forensically imaged/copied by an unauthorized individual. Accordingly, there is little to no risk of harm, and therefore notice need not be provided.

d. Mitigation of the Risk Following Unauthorized Disclosure

Consider the extent to which the risk of harm from unauthorized access to the PII in question has been mitigated by the entity that suffered the security incident (as compared to mitigation efforts the affected individuals might employ). For example, consider whether the PII Controller has obtained the recipient's assurances that the PII will not be further used or disclosed (through a confidentiality agreement or similar means), has been completely returned, or has been/will be destroyed. This factor, when considered in combination with the nature of the unauthorized recipient, may lead to a determination that the requisite risk of harm has not been established provided that the recipient is able to be identified, and legal action can be brought against the recipient, if necessary. For example, an entity may be able to obtain and rely on the assurances of an employee, affiliated entity, or vendor that they destroyed the information in order to make such a determination. However, such assurances from other third parties may not be sufficient to overcome other indicia that the requisite risk of harm exists.

3. Advantages of the Two-Tiered PII Approach

The flexible approach to defining PII encourages PII Controllers to address the risk of harm in a proactive way. They can consider what forms of PII they are responsible for safeguarding, assess whether a compromise of that information could conceivably give rise to a risk of harm, and then make decisions as to the appropriate levels of safeguards to protect that PII.

Under the *Commentary's* proposal, a PII Controller that has experienced a Security Breach involving Category I PII may seek to determine as to any PII Subject associated with the PII in question whether the Security Breach as to that associated PII is unlikely to have caused and is unlikely to cause harm to the PII Subject; unless it makes such a determination, the PII Controller is required to give notice of the Security Breach to that PII Subject. However, whether other PII (such as subscription to a magazine or membership to an organization) is sufficiently sensitive depends on contextual considerations, such as the nature of the magazine, or the PII Controller and the nature of the PII. For example, a membership list for Alcoholics Anonymous may be sufficiently sensitive, whereas a membership list for a "dog lovers" organization may not be. The potential risk of harm from unauthorized access to information showing the names of members of Alcoholics Anonymous is evident. Accordingly, under the *Commentary's* proposal, a PII Controller that has experienced a Security Breach involving Category II PII must determine as to any PII Subject associated with the PII in question whether the Security Breach as to that associated PII is likely to have caused or is likely to cause harm to the PII Subject and, if it makes such a determination, is required to give notice of the Security Breach to that PII Subject.

This context-specific analysis may incentivize PII Controllers to engage in PII analysis prior to a breach. Such analysis promotes consideration of privacy issues in a preventive manner, rather than a reactive one, and informs the PII Controller's assessment of the required safeguards.

E. Elaboration on the Effect of Encryption and De-identification

Existing breach notification statutes recognize that some data security incidents may have no practical consequences because the accessed data is either not accessible to or usable by anyone other than its owner, or it is not likely to be capable of

being associated with an individual or household. In effect, this means that no data breach affecting PII has occurred in the first instance, much less is any harm to an individual likely. Thus, if the data that was disclosed without authorization is encrypted, de-identified, or otherwise rendered inaccessible or not attributable to any individual, there is no reasonable likelihood of harm, and the incident is not a breach requiring notification. Differing treatments of encrypted and de-identified information create confusion and inconsistent outcomes when it comes to data breach notification.

1. Encryption Is Already a Recognized Safe Harbor but Not Well-Defined

As discussed above, "Encryption" for purposes of the Model Data Breach Notification Law proposed in this *Commentary* broadly means: "a technology for securing computerized data in such a manner that it is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key, which is not accessible by unauthorized persons." More specifically, encryption is the process of using an algorithm to transform information to make it unreadable in its original format for unauthorized users. This cryptographic method protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text. This encoded data may only be decrypted or made readable with a key. Symmetric-key and asymmetric-key are the two primary types of encryption.

Most states' data breach notification statutes provide for an exception to the requirement to notify individuals of a data breach involving their PII if the data exposed to unauthorized access was encrypted. California, for example, provides for this exception in requiring notification to residents:

> (1) whose unencrypted PII was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted PII was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that PII readable or useable.[36]

The data breach notification statutes of other states, like Illinois, simply remove encrypted data from the definition of "PII" altogether, the consequence of which is that unauthorized access to encrypted data does not constitute a data breach in the first place:

> "Personal information" means either of the following: "(1) An individual's first name or first initial and last name in combination with any one or more of [several listed] data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security; . . . [or] (2) User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or

36. CAL. CIV. CODE § 1798.29(a).

> unredact or otherwise read the data elements have been obtained through the breach of security."[37]

The *Commentary* believes an exclusion from breach notification requirements for encryption-protected PII is appropriate, and it further believes the clearest mechanism for implementing such an exclusion is by means of a separate statutory provision rather than by building such an exclusion into the definition of "PII" or "Security Breach." Accordingly, the Model Data Breach Notification Law proposed in this *Commentary* includes a separate provision to implement an exclusion from breach notification requirements for PII that is protected by encryption via generally accepted industry standards.[38]

2. Many Existing Data Breach Laws Do Not Account for De-identification

The intent of information sanitization, e.g., data anonymization and pseudonymization, is privacy protection by de-identification. It is the process of either encrypting or removing PII from data sets, so that the people whom the data describe remain anonymous and are not reasonably capable of being identified. The GDPR strongly suggests that, where possible, stored data on people in the European Union undergo either an anonymization or a pseudonymization process. Similarly, section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information.[39] Under this standard, health information is not individually identifiable if it

---

37. 815 ILL. COMP. STAT. § 530/5.

38. If, however, the PII Controller later learns or determines that the encryption was defeated or the PII otherwaise was not de-identified or protected by encryption, then the exclusion would not apply, and the PII Controller should revisit the breach notification analysis recommended by this *Commentary*.

39. 45 C.F.R. § 164.514.

does not identify an individual, and if the covered entity has no reasonable basis to believe it can be used to identify an individual.

Pseudonymization is a data management and de-identification procedure by which PII fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. A single pseudonym for each replaced field or collection of replaced fields makes the data record less identifiable while remaining suitable for data analysis and data processing. The process of obscuring data with the ability to reidentify it later is also called pseudonymization and is one way organizations can store data in a way that is HIPAA compliant. Note that the GDPR recitals point out that pseudonymized data is still personal data because as long as the key exists and has not been destroyed, there is always the chance that the data could be compromised.

An exclusion from breach notification requirements for PII that is protected by de-identification is appropriate—provided that the breached entity can confirm that the threat actor does not have access to the key or other information sufficient to identify the individual. The clearest mechanism for implementing such an exclusion is by means of a separate statutory provision, rather than by building such an exclusion into the definition of "PII" or "Security Breach." Accordingly, the Model Data Breach Notification Law proposed in this *Commentary* includes an exclusion for PII protected by de-identification as part of the separate provision being proposed to implement an exclusion from breach notification requirements for PII that is protected by encryption.

F. How Should Notice Be Provided; Who Should Provide It; and What Should It Look Like?

1. Current Data Breach Notification Laws Provide the Following Regarding what Constitutes Acceptable Notice

The U.S. state data breach notification laws vary in terms of appropriate methods of notification, but all states give written notice via U.S. mail as at least one option. Often, written notice is framed as the first option in combination with other possible options (such as telephonic notice or electronic notice). Most states have an option for substitute notice, which is triggered by: (i) the cost of notification exceeding a certain threshold, (ii) the number of individuals affected exceeding a certain threshold, or (iii) the organization lacking appropriate contact information. Electronic or email notification is usually a form of substitute notice under most state statutes. Substitute notice often requires more actions than standard notice, as it generally requires, in addition to notice by email, posting to the organization website, and notification to statewide media.

If email is given as an option for notice, it is often limited in the following ways:

- Electronic notice, for those persons for whom it has a valid email address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001;[40] or

40. *See, e.g.*, CONN. GEN. STAT. § 36a-701b(e); MISS. CODE ANN. § 75-24-29(6); MO. REV. STAT. § 407.1500(2)(6)(b).

- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001;[41] or
- Email notice, if a prior business relationship exists and the person or entity has a valid email address for the individual.[42]

2. Compliance with the Current Methods of Notification Can Be Problematic

Providing written notice via U.S. mail can be very costly, particularly for small and midsize organizations. Most state laws have substitute notice provisions, which should provide a cheaper alternative to written U.S. mail notice. However, the available substitute notice provisions are often triggered by individual thresholds so high that they are not accessible to most organizations. In addition, though substitute notice may seem less costly on the surface, a closer look at most states' provisions reveals a surprising lack of cost savings. Substitute notice allows a cheaper notification method (such as email), but only in conjunction with relatively expensive notification methods (such as statewide media notification). Since data breaches will likely affect most PII Controllers of varying levels of sophistication and size, it is problematic to make notice expensive or difficult. Complicated and costly methods of notification will not accomplish the broader goal of data breach notification, which is to alert individuals to enable them to protect themselves.

41. VT. STAT. tit. 9 § 2435(b)(6)(A)(ii)(II).

42. 73 PA. STAT. § 2302(3).

3. Considerations to Address Issues with Notification Methods

The overarching purpose of state data breach notification laws is to provide prompt notice to individuals to permit them to take action to protect themselves against whatever harm they have been exposed to by the event in question. As such, a model method of notification should be simple and low cost, which will allow PII Controllers to accomplish this task quickly.

To that end, the *Commentary*'s proposed Model Data Breach Notification Law provides that PII Controllers should be able to provide notice through traditional U.S. mail or email—provided that the PII Controller already communicates with the individual through email. Email is the primary mode of communication for most individuals today, and one that most individuals can be relied upon to check regularly. Many PII Controllers will have current email addresses of their customers. If PII Controllers already communicate with individuals via email, or if the customer has given their email address through the course of their business relationship, communicating through email gives notice to individuals quickly and effectively.

The *Commentary*'s proposed Model Data Breach Notification Law further provides that if a PII Controller does not have access to the U.S. mail or email of each PII Subject, the PII Controller should post notification of the Security Breach for at least 60 days on the PII Controller's website, if the PII Controller maintains one. This post should consist of a link to the notice on the home page or first significant page after entering the website. The link should be in larger or contrasting type, font, or color to surrounding text or set off from other text by symbols or marks that call attention to it.

4. Who Should Send Notice?

The *Commentary*'s proposed Model Data Breach Notification Law provides that if a PII Controller experiences a Security Breach, conducts an investigation in accordance with Section IV.B of the *Commentary* and determines that the breach likely caused or is likely to cause harm to one or more of the PII Subjects associated with the PII in question, then the PII Controller should provide notice of the Security Breach to each PII Subject as to whom the PII Controller made such determination.

Where an obligation to provide notice of a Security Breach to a PII Subject exists under this Section IV.D of the *Commentary*, the proposed Model Data Breach Notification Law provides that such notice should be provided either by the PII Controller or by another party that has an agreement with the PII Controller that requires the party to provide such notice.[43] It is common for PII Controllers to share information related to PII Subjects with service providers and other contract partners. For example, a business may provide human resources data relating to its employees to its benefits provider, or a customer-facing business may provide customer preferences to a market research company. When a Security Breach occurs in this type of situation, the parties should "have the flexibility to set forth specific obligations for each party, such as who will provide notice to individuals . . . , following a breach . . ., so long as all required notifications are provided."[44] The parties could set forth in their

43. There are, of course, some exceptions—such as if the PII Controller was required to provide such notice under an agreement, but the relationship between the PII Controller and the other party terminated, and the PII Controller no longer has access to the data to provide such notice.

44. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan.

underlying agreement who is responsible for providing notice to impacted PII Subjects. In addition, the parties should determine which entity is in the best position to provide notice to the individual, by considering among other things: (1) which functions the service provider or contract partner performs on behalf of the entity; (2) which entity has the relationship with the individual; and (3) which entity has access to information to provide such notice.[45] Parties should take steps to ensure that the individual does not receive notifications from both the PII Controller and the service provider about the same breach, which may create confusion.[46] The PII Controller remains responsible for ensuring that notice of the Security Breach is provided, either by itself or by its service provider or contract partner.

G. What Should Be the Timeline for Notification?

1. General Issues Affecting the Timing of Data Breach Notification to Individuals

Not all threats to data security result in the unauthorized access to PII held by a PII Controller, and therefore are not security breaches as defined by statute. The legal determination of a Security Breach can only occur after gathering and analyzing relevant facts. It may take time to understand the underlying events and arrive at the legal conclusion of a Security Breach. Accordingly, the affected individuals could have been suffering harm for some time before they receive notice of the event that is causing such harm.

25, 2013) (to be codified at 45 C.F.R. §§ 160, 164), *available at* https://www.federalregister.gov/d/2013-01073.

45. *Id*.

46. *Id*.

Several factors[47] contribute to the amount of harm affected individuals may suffer from a Security Breach, including, (a) whether the underlying Security Breach is ongoing, (b) what steps the PII Controller that suffered the Security Breach can take to mitigate harm to affected individuals, and (c) what steps affected individuals themselves can take to mitigate harm from the Security Breach, in spite of timing issues resulting from the investigation of any breach, or the failure to detect the breach. Reducing harm through each of these factors reveals an inherent tension between the costs and benefits of however much time elapses between the occurrence of the Security Breach and the provision of notice about the breach. On the one hand, with more information about the Security Breach, the PII Controller and the individuals whose PII was accessed in the breach can respond more precisely and thoroughly to the specific threat posed by the breach. On the other hand, gathering all the relevant information about a Security Breach takes time, and during that time, individuals whose PII was accessed could suffer increasing harm. The more harm individuals suffer, the greater a PII Controller's potential legal liability for that harm.

2. Current Data Breach Notice Timing Requirements

State breach notice statutes generally employ one of three different approaches to balancing the timing of Security Breach notifications with the information content of Security Breach notifications to affected individuals:

47. Other relevant factors include the sensitivity of the breached data, the value of the breached data on the black market, and whether the PII qualifies for special statutory protections. Discussion of these factors and how they impact the harm suffered by affected individuals is beyond the scope of these guidelines.

i. Notification to impacted individuals must be made without unreasonable delay or in the most expedient time possible

The timing for notification in this approach emphasizes promptness but allows for the time necessary to gather relevant information. For example, prompt notice to affected individuals may allow them to take steps on their own to mitigate the harm from a Security Breach, but the PII Controller may not have had time to determine whether the breach is still ongoing. By contrast, waiting to provide notification to affected individuals until the breach has been stopped and a tailored risk mitigation plan has been implemented may only marginally reduce the potential harm to affected individuals.

Depending on the specific nature of the breach, the best way to minimize the harm to the affected individuals (and accordingly, the potential liability to the PII Controller) may be to provide notifications as soon as the breach is discovered. For example, if a rogue employee gained unauthorized access to PII, once the employee can no longer gain access to the PII, the risk of harm is effectively eliminated. In the case of mass exploits like the Heartbleed Bug,[48] the individual's and PII Controller's harm mitigation efforts would likely have little effect until the underlying issues in the software are patched. Accordingly, notifications to affected individuals would make the most sense once the underlying security threat has been addressed thoroughly.

With this timing-of-notification standard, the specific facts of the Security Breach dictate whether the PII Controller provided notifications promptly enough. Barring a statutory liability for notification delays, the affected individuals would likely need to realize harms from the Security Breach or the delay in

48. Timothy B. Lee, *The Heartbleed Bug, explained*, VOX (May 14, 2015), https://www.vox.com/2014/6/19/18076318/heartbleed.

notification in order for the PII Controller to incur liability. This timing-of-notification standard generally leaves the courts in the best position to quantify harms and apportion liability. Some states with this timing standard include California,[49] New York,[50] Massachusetts[51] and Illinois.[52]

It appears that without a set deadline, many PII Controllers argue that as long as a good-faith investigation into the breach is ongoing, they do not need to provide notice to affected individuals. Though this approach might match the letter of the law, it defeats the spirit of the law that aims to help individuals protect themselves.

ii. Notification to impacted individuals must be made without unreasonable delay or in the most expedient time possible *and* specify a deadline for notice

This approach largely uses the same standard described in approach (i). However, this approach adds the caveat that no more than a specified number of days can pass between the date a Security Breach is discovered and the date affected individuals receive notification of the breach. In Colorado, for example, the notification requirement reads as follows:

> Notice must be made in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the

49. CAL. CIV. CODE § 1798.29(a).

50. N.Y. GEN. BUS. LAW § 899-AA(2).

51. MASS. GEN. LAWS. Ch. 93H, § 3.

52. 815 ILL. COMP. STAT. § 530/10(a).

> breach and to restore the reasonable integrity of the computerized data system.[53]

Like approach (i), the specific facts of a Security Breach can generally dictate whether expediency or details about the information involved in the breach should be prioritized in the notification to affected individuals. Assuming the PII Controller is working diligently, though, there may be occasions when all the necessary information about the Security Breach is not yet available but notifications are required. Accordingly, the notification's ability to help prevent further harm to the affected individuals would be diminished. The deadline for notice under such circumstances could appear arbitrary.

If a PII Controller does not work diligently in response to a Security Breach, the deadline could act as a "safe harbor." PII Controllers may respond to security breaches in such a manner that they meet the statutory deadline, even if the circumstances of the Security Breach merit a speedier notification. In such cases, affected individuals could realize increased harm for which the PII Controller might not be held liable because it met the statutory deadline.

This approach sets a standard for what constitutes timely notice. Therefore, it takes an important step in protecting affected individuals, even if PII Controllers suffering a breach have to operate with incomplete information at the time of the notification.

The facts of security breaches can be difficult to ascertain. Quantifying the harms realized by affected individuals has proved challenging, and apportioning the associated liability has stretched the abilities of the courts. This time-of-notification standard could shift some liability away from PII Controllers

53. COLO. REV. STAT. § 6-1-716(2)(a).

that need to provide notice of security breaches at the expense of affected individuals.

iii. Simply specify a deadline for notice

This standard for the timing of Security Breach notification simply states that no more than a set number of days can pass between the date a Security Breach is discovered and the date affected individuals receive notification of the breach. South Dakota is an example of this, mandating a sixty-day deadline.[54] PII Controllers working diligently in response to a breach will work to provide the right information to affected individuals as quickly as possible. However, like approach (ii), when PII Controllers are not prepared to provide an appropriate notification by the deadline, the deadline can seem arbitrary.

Unlike approach (ii), this timing of notification standard does not require PII Controllers to provide notifications without unreasonable delay (or as quickly as possible). By setting a hard deadline, though, PII Controllers are required to act in what is deemed a timely manner. The breach notice statute effectively treats all security breaches the same for the purpose of timing of notifications. Even when the facts of Security Breach merit a very speedy notice to affected individuals, PII Controllers have no incentive to provide notifications any time sooner than the deadline.

This timing-of-notification standard can help promote judicial efficiency. The question of whether the PII Controller's timing of breach notification contributed to an individual's harm would not have much traction under such a statutory construction. Accordingly, this timing-of-notification standard could shift liability away from PII Controllers that need to provide notice of security breaches at the expense of affected individuals.

54. S.D. CODIFIED LAWS § 22-40-20.

All three timing-of-notification standards have their advantages and disadvantages. A uniform standard should allow for the greatest flexibility in the timing of Security Breach notifications, while incentivizing diligent responses from PII Controllers

H. Under What Circumstances Should Credit Monitoring Be Offered?

Credit monitoring services "scan activity that shows up on your credit reports" and "usually alert you when" new activity shows up on your credit report.[55] Credit monitoring alerts affected individuals *after* someone has applied for or opened new credit in their name. "Credit monitoring can be helpful in the case of a Social Security number breach," but "[i]t does not alert you to fraudulent activity on your existing credit or debit card account."[56] The timing of the alerts received in connection with credit monitoring is problematic as well. An individual learns *after the fact* of unauthorized use of PII. As one industry expert stated, "by the time you get the alert, it's too late, the damage has been done. It just shortens the time to detection so you may have a slightly improved chance of cleaning up damage faster."[57]

Importantly, however, many consumer finance experts recommend that individuals both freeze their credit and regularly check their credit reports after any data breach to determine if

---

55. *What to Know About Identity Theft*, FED. TRADE COMM'N (April 2021), https://consumer.ftc.gov/articles/what-know-about-identity-theft.

56. Cal. Dep't of Justice, Breach Help: Consumer Tips from the California Attorney General, Consumer Info. Sheet 17 (Oct. 2014), at 1, *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis-17-breach-help.pdf.

57. *Are Credit Monitoring Services Worth It?*, KREBS ON SECURITY (March 19, 2014), https://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/ (quoting Avivah Litan, a fraud analyst with Gartner Inc.).

any fraudulent activity has occurred so that it can be quickly remediated.[58] While credit monitoring has some weaknesses, its service provides consumers with alerts when their credit files have changed, which is consistent with advice from agencies advising consumers to regularly check their credit files.

1. Credit Monitoring and State Breach Notification Laws

Despite some of the inherent weaknesses with credit monitoring, four states[59] have credit monitoring requirements in connection with their state data breach notification laws. In 2014, California amended its breach notification law as follows:

> If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed PII defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).[60]

58. This same guidance is recommended by the Federal Trade Commission. *See* FEDERAL TRADE COMMISSION, DATA BREACH RESPONSE: A GUIDE FOR BUSINESS, *available at* https://www.ftc.gov/system/files/documents/plain-language/560a_data_breach_response_guide_for_business.pdf (last visited Aug. 2, 2024); *When Information Is Lost or Exposed*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/#/Info-Lost-or-Stolen (last visited Aug. 2, 2024).

59. CAL CIV. CODE § 1798.82(d)(2)(G); CONN. GEN STAT. § 36a-701b(b)(2)(B); DEL. CODE. tit. 6 § 12B-102(e); MASS. GEN. LAWS ch. 93H § 3A(a).

60. CAL CIV. CODE § 1798.82(d)(2)(G).

California's law states that identity theft protection services should be used for breaches involving Social Security numbers, driver's license numbers, California identification card numbers, tax identification numbers, passport numbers, military identification numbers, or other unique identification numbers issued on government documents commonly used to verify the identity of a specific individual. Noticeably excluded from the types of PII where identity theft protection should be offered under California law are breaches involving account, credit card, or debit card numbers in combination with any required security code, access code, or password that would permit access to an individual's financial account, medical information, health insurance information, information or data collected through the use or operation of an automated license plate recognition system, and genetic data.[61]

In 2015, Connecticut followed California and passed a law affirmatively requiring "appropriate identity theft prevention services and, if applicable, identity theft mitigation services" for at least one year. It is important to note that the Connecticut law, like the California law, does not require credit monitoring in all cases, but instead requires "appropriate identity theft prevention services." Connecticut Attorney General George Jepsen added the following in connection with the announcement of the new Connecticut law:

> The bill also calls for companies who experience breaches to provide no less than one year of identity theft prevention services. This requirement sets a floor for the duration of the protection and does not state explicitly what features the free protection must include. I continue to have enforcement authority to seek more than one year's protection—and to seek

61. *Id.*, §§ 1798.82(d)(2)(G); 1798.82(h)(1)(C)-(H).

> broader kinds of protection—where circumstances warrant. Indeed, in matters involving breaches of highly sensitive information, like Social Security numbers, my practice has been to demand two years of protections. I intend to continue to that practice.[62]

Effective October 1, 2018, Connecticut increased its credit monitoring requirement from 12 months to 24 months for residents who experience a Security Breach affecting Social Security numbers.[63]

Delaware's breach notification law is more limited than California's, as it requires credit monitoring only in breaches involving Social Security numbers. Specifically, the Delaware law states the following:

> If the breach of security includes a Social Security number, the person shall offer to each resident, whose personal information, including Social Security number, was breached or is reasonably believed to have been breached, credit monitoring services at no cost to such resident for a period of 1 year. Such person shall provide all information necessary for such resident to enroll in such services and shall include information on how such resident can place a credit freeze on such resident's credit file.[64]

On January 10, 2019, Massachusetts Governor Charlie Baker signed legislation that became effective on April 11, 2019, that

---

62. Press Release, Statement from AG Jepsen on Final Passage of Data Breach Notification and Consumer Protection Legislation, State of Connecticut (June 2, 2015), https://portal.ct.gov/AG/Press-Releases-Archived/2015-Press-Releases/Statement-from-AG-Jepsen-on-Final-Passage-of-Data-Breach-Notification-and-Consumer-Protection-Legisl.

63. CONN. GEN STAT. §36a-701b(b)(2)(B).

64. DEL. CODE. tit. 6 § 12B-102(e).

requires an offer of complimentary credit monitoring for "a period of not less than 18 months" when the data security incident involves a Massachusetts resident's Social Security number.[65]

2. Identity Theft Mitigation/Recovery Services

In 2014, the Federal Trade Commission estimated that the average identity theft victim spent more than 200 hours across 18 months resolving their issues with credit-reporting agencies.[66] For this reason, identity theft recovery services provide a significant value to individuals who have been victimized by identity theft. Both California and Connecticut implicitly recognize this value by referring to identity theft mitigation services in connection with their respective laws.

Identity recovery services typically provide trained counselors to help individuals work through the fraud resolution process after receiving notice of a breach. The counselors can assist with writing letters to creditors and debt collectors to dispute unauthorized charges and close accounts, "plac[ing] a freeze on your credit report to prevent an identity thief from opening new accounts in your name, or guid[ing] you through documents you have to review."[67] Some services will represent individuals in dealing with creditors or other institutions if formally granted authority to act on the individual's behalf.[68] Others may help individuals place fraud alerts with the consumer reporting agencies and government agencies. These kinds of services can be extremely valuable, especially given the amount of time and effort individuals can spend in addressing issues associated

65. MASS. GEN. LAWS ch. 93H § 3A(a).

66. *Latest Data Breach Spotlights Need for Identity Restoration*, BUSINESSWIRE (Oct. 7, 2015), https://www.businesswire.com/news/home/20151006006149/en/Latest-Data-Breach-Spotlights-Identity-Restoration.

67. *Id*.

68. *See id*.

with fraudulent use of name,[69] Social Security number, and account information. For this reason, it is imperative that any state law requirement for credit monitoring include a requirement that the breached entity provide identity restoration services.

Individuals who have been the victim of a data breach may realize some benefits from credit monitoring but will realize significantly enhanced benefits from having both monitoring and comprehensive identity theft mitigation resources available to them. It is for this reason that the proposed model language combines credit monitoring with comprehensive identity theft prevention and mitigation/restoration services.

In certain incidents, Dark Web scans can be bundled with credit monitoring and identity restoration services to offer more comprehensive coverage to individuals. The scans can search known web pages on the Dark Web for Social Security numbers, email addresses, phone numbers, or medical information. Because Dark Web scans are only "a point in time," regular, repeated scans are essential for this service to be effective.

Given the above considerations, the *Commentary* recommends that if credit monitoring services are provided as a result of a Security Breach, breached entities should also consider services that include Dark Web monitoring and identity restoration to provide enhanced protections to individuals who were impacted by any Security Breach.

---

69. "[Identity theft] victims reported spending an average of about 7 hours clearing up the issues. Victims of existing credit card account misuse spent an average of 4 hours resolving problems, while victims who experienced multiple types of identity theft with existing accounts and other fraud spent an average of 24 hours resolving all problems." ERIKA HARRELL, VICTIMS OF IDENTITY THEFT, 2014, U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE STATISTICS (Rev. Nov. 13, 2017), at 10, *available at* https://bjs.ojp.gov/content/pub/pdf/vit14.pdf.

I. How Should PII Controllers Be Expected to Notify Law Enforcement and Regulatory Authorities?

The state statutes requiring affected entities to notify law enforcement or regulatory authorities vary widely and lack uniformity. They contain not only widely diverging timeframes for notice but also require notice to different governmental entities under different circumstances. Notably, state notification statutes generally do not require notification to criminal law enforcement authorities. The statutes are uniform, however, in one unfortunate respect: none requires notice to the FBI, the U.S. Secret Service, or the Department of Homeland Security—the three entities principally responsible for combatting cyber threats and other actors driving the number of data breaches across the nation.

1. Various Statutes Requiring Notification to a Law Enforcement Entity

The majority of states and Puerto Rico require notice to some governmental entity. These entities include Attorneys General, consumer protection entities, divisions of the state police, and insurance regulators in the event of breaches involving an insurance company. Notably, California requires notice to different state entities depending on the nature of the breach.

The circumstances giving rise to notification also differ among the states. For example, below is a list of various differences amongst state statutes.

- *No numerical threshold of individuals impacted*—Connecticut, Idaho, Indiana, Louisiana, Maine, Maryland, Massachusetts, Montana, Nebraska, New Hampshire, New Jersey, New York, North Carolina, Puerto Rico, Texas, Vermont;
- 50 or more individuals affected—District of Columbia;

- *250 or more individuals affected*—North Dakota, Ohio (if insurance entity), Oregon, Texas, South Dakota, Illinois (if a breach by a state agency occurs), Kentucky (if insurance licensee);
- *500 or more individuals affected*—California, Colorado, Delaware, Florida, Illinois, Iowa, Rhode Island, Utah, Washington;
- More than 500 individuals affected—Minnesota;
- *1000 or more individuals affected*—Alabama, Arizona, Arkansas, Hawaii, Missouri, New Mexico, South Carolina, Virginia.

Notification time thresholds also vary:

- *24 hours*—Idaho (if a public agency experiences a data breach);
- *72 hours*—New York (if entity subject to regulation by Department of Financial Services), South Carolina (if insurance licensee);
- *10 days*—Puerto Rico, Michigan (if insurance industry), New York (if educational agency);
- 14 business days—Vermont;
- *15 business days*—California (if medical information involved);
- *30 days*—Colorado, Florida, Maine, Texas, Washington;
- *45 days*—Alabama, Arizona, Arkansas, Indiana, Maryland, New Mexico, Oregon;
- *60 days*—Connecticut, Delaware, Louisiana (timely if received within 10 days of individual notice), South Dakota.

Even where not explicitly required by statute, it is a best practice in the industry to submit notifications to government

entities contemporaneous with or prior to notifications to individuals.

Meanwhile, several states specify the information that affected entities must include in the notice to the governmental entity: Alabama, California, Colorado, Connecticut (insurance entity), Delaware (insurance licensees), District of Columbia, Florida, Hawaii, Illinois, Kentucky (insurance licensee), Louisiana, Maine (insurance entity), Maryland (insurance carrier), Massachusetts, New Hampshire, New Mexico, North Carolina, Oregon, Rhode Island, South Carolina, Vermont, and Washington.

2. Criminal Law Enforcement Notification

As a general matter, state data breach statutes appear to focus on the importance of notifying regulators or state attorneys general offices rather than criminal law enforcement authorities. Indeed, few state data breach notification statutes require notifying criminal law enforcement agencies. Although regulatory authorities and civil enforcement actions can play a role in encouraging private industries to adequately protect consumer data, criminal law enforcement authorities play a critical role in exposing, deterring, and incapacitating cyber-criminal threat actors that attack U.S. organizations in the first instance.

While at least two states require notification to the state police,[70] the lion's share of cyber-criminal investigations and prosecutions is conducted by the U.S. Department of Justice, the Federal Bureau of Investigation, the U.S. Secret Service, and to some extent, the Department of Homeland Security. While state and local law enforcement agencies play an important role in combatting events that give rise to data breaches, the interstate and international character of cyber-criminal conduct imposes

70. N.J. REV. STAT. § 56:6-163(c)(1); N.Y. GEN. BUS. LAW § 899-AA(2), 8(a).

limits on the ability of state and local law enforcement to adequately address the threat.

3. Regulatory Notification or Civil Enforcement Notification

As noted above, a number of jurisdictions require notification, often in very short order, to a regulator or a state entity with the authority to initiate a civil enforcement proceeding, a regulatory action, or to impose fines. Indeed, the GDPR requires regulatory notification within 72 hours unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons."

Consideration should be given to the purpose of requiring such notifications, especially on such a swift time horizon. There may be little benefit to requiring a PII Controller to notify a regulator or civil enforcement authority before a PII Controller has had time to sufficiently identify the salient facts of a data breach. Indeed, many forensic investigations into a data security incident can proceed for several weeks before a PII Controller has an appropriate handle on the scope of the problem. Given the limited ability of regulatory and civil enforcement authorities to affirmatively assist a PII Controller impacted by a data security incident, it may be more useful to provide a PII Controller with reasonable time for providing a detailed notice to a regulatory or civil enforcement authority, i.e., requiring at least 30-45 days. This approach would also have the benefit of avoiding multiple rounds of notice to regulators, and thereby avoiding inundating a governmental authority with new information every time a forensic investigator uncovered a previously unknown fact, especially where a risk-averse PII Controller may be concerned about the appearance of "hiding" information.

Whatever the timetables requiring notification, care should be taken to create parity with the requirement for notifying impacted individuals.

4. The Notification to Multiple Regulators

The challenges of notifying multiple regulatory authorities are a pervasive problem for PII Controllers impacted by a data breach involving a wide swath of data belonging to individuals located in a wide swath of states. Overlapping notification requirements add to the costs of data breaches and impose additional burdens on entities in the midst of what is often a fast-moving crisis.

One solution may be to create a centralized notification system that gives an affected entity the ability to provide notice via an online portal; ideally, the system would be accessible by the different state regulators. One model may be the Federation of Tax Administrators ("FTA"), which serves as the principal state tax administrators of the 50 states, the District of Columbia, New York City and Philadelphia. When a business or tax professional identifies it has been the victim of a data breach, it can notify the FTA by sending an email to StateAlert@taxadmin.org, with a single process at no charge.

Given the above considerations, the *Commentary* recommends that if an obligation exists pursuant to the Model Breach Notification Statue to provide notice of a Security Breach to a PII Subject, then such notice shall also be provided simultaneously to a state or federal regulatory authority, and that the state enacting language consistent with this model statute should establish a centralized reporting mechanism available via the internet.

IV. PROPOSED MODEL DATA BREACH NOTIFICATION LAW

This section sets forth the *Commentary*'s proposed Model Data Breach Notification Law in its entirety.

A. Definitions as used in this section, the term:

1. **"Access"** means the unauthorized viewing, disclosure, acquisition, or exfiltration of data, however accomplished, whether by human interaction, automated process (e.g., malware), or other, and whether occurring deliberately, through negligence, innocently, or otherwise.

2. **"Category I PII"** is PII where a Security Breach involving Category I PII triggers notice unless a PII Controller's investigation determines that the Security Breach is unlikely to cause Harm. Category I PII is PII where an individual's first name, or first initial, and last name is in combination with and linked to any one or more of the following data elements:

a. Social Security number;

b. motor vehicle operator's license number or government identification card number;

c. financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords to access the financial account;

d. account passwords or personal identification numbers or other access codes for a financial account;

e. biometric information, including a fingerprint, retinal scan, and facial recognition data, and genetic information;

f. health information about sensitive diagnoses, including HIV, STDs, substance abuse, or mental health;

g. login credentials (including but not limited to email address or username, in combination with password or other access code such as a personal identification number ("pin" or "pin number")).

3. **"Category II PII"** means PII where the PII Controller must evaluate the possibility of the PII impacted by the Security Breach causing Harm to the PII Subject(s), because the information breached may not be Category I PII, but unauthorized access to the PII may still cause Harm to the PII Subject. Examples of Category II PII include, but are not limited to:

a. date of birth;

b. maiden name of the individual's mother;

c. digitized or other electronic signature;

d. passport number;

e. insurance information (identification numbers, insurance policy numbers, or any other unique identifying number);

f. health information that is not sensitive diagnosis information (health history, information about illnesses, information, or observations about a patient, etc.);

g. employee personnel files or similar evaluations or personal commentary (subjective or objective employee performance metrics, any kind of personal analysis, goals that might be about an identifiable individual, etc.);

h. physical asset information that consistently links an item to an individual (MAC address, IP address, car license plate number, home address);

i. geolocation data (data used on ride-sharing apps, augmented reality apps or games);

j. customer loyalty or affinity account numbers;

k. physical asset or software usage data (browser history, cookies, software tokens, usage metadata, etc.);

l. data concerning a person's sex life or sexual orientation;

m. political affiliations, donations, or beliefs held related to political or social topics;

n. information gathered for the specific purpose of allowing an individual to reset his or her password or account credentials;

o. any other unique number-based code or characteristic that is about an identifiable individual (phone number, an organizational anonymized code for an individual, etc.).

4. **"De-identified"** means there is no reasonable basis to believe the data is capable of identifying or being associated with a particular individual or household.

5. **"Encryption"** means a technology for securing computerized data in such a manner that it is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key, which is not accessible by unauthorized persons.

6. **"Harm"** means physical injury, financial loss or damage (including but not limited to financial loss or damage from identity theft or other fraud or misuse, or from loss of financial or educational opportunity), and serious and prolonged emotional injury (including but not limited to distress, embarrassment, humiliation, or loss of reputation). The fact that a circumstance constitutes "Harm" pursuant to this statute shall have no bearing on a party's ability to bring suit against an entity related to a Security Breach, or a court's jurisdiction over such a suit based on such circumstance.

7. **"Notice"** means communication to PII Subjects in the event of a Security Breach. Such Notice shall be in the format of Appendix A hereto, or substantially similar.

8. **"Personally Identifiable Information"** ("PII") means information, whether recorded in electronic or hard copy form or not, about, or pertaining to, or traceable to, either alone or in combination with other information, an identifiable individual.

9. **"PII Controller"** means any entity, including a government entity, that collects, receives, maintains, possesses, controls, or has custody of PII.

10. **"PII Subject"** means any individual to whom PII relates.

11. **"Security Breach"** means a circumstance that leads a PII Controller to believe or would lead a reasonable PII Controller to believe that Access to PII has occurred as to PII that it maintains, controls, or has custody, where the PII is neither Encrypted nor De-identified .

B. Risk of Harm

Any PII Controller that has experienced a Security Breach involving Category I PII may seek to determine as to any PII Subject associated with the PII in question whether the Security Breach as to that associated PII is unlikely to have caused and is unlikely to cause Harm to that PII Subject.

Any PII Controller that has experienced a Security Breach of Category II PII shall determine as to each PII Subject associated with the PII in question whether the Security Breach as to that associated PII has likely caused or is likely to cause Harm to that PII Subject.

In determining whether a Security Breach has likely caused or is likely to cause, or is unlikely to have caused and is unlikely to cause, such Harm, the PII Controller shall consider:

- the nature, extent and sensitivity of the PII;
- the extent to which the data integrity or availability of the PII to the PII Subject may have been adversely impacted;
- the identity of the person who Accessed the PII without authorization;
- the likelihood that the PII has been or will be misused in a manner resulting in Harm;

- whether the risk that the PII would be misused in such a manner has been mitigated following its unauthorized Access;
- the type of breach (e.g., whether a fraudulent third party is involved) and the likelihood of misuse;
- ease of identification of individuals (is full name present, or are they well known);
- severity of consequences for individuals arising from misuse of their information (e.g., financial fraud, identity fraud, physical harm or distress); and/or
- special characteristics of the individuals (e.g., elderly, children, or vulnerable categories of individuals)

If a PII Controller that has experienced a Security Breach determines, after conducting an investigation permitted or required by this Section, that it has no obligation under Section D to provide notice of the Security Breach to one or more of the PII Subjects associated with the PII in question, the PII Controller shall make and preserve a record of its investigation and determination for production to any regulator when requested.

C. Effect of Encryption, De-identification, and Similar Technologies

Access to PII does not constitute a Security Breach if the PII has been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of an effective technology or methodology or has otherwise been made not reasonably capable of being associated with an individual or household. For example, a Security Breach has not occurred if (i) the PII is Encrypted, anonymized, pseudonymized, or De-identified; and (ii) the Encryption key and/or reidentification key likely has not been acquired by the unauthorized person; and (iii) the PII is not otherwise likely capable of de-anonymization, de-pseudonymization, or reidentification by an unauthorized person.

D. Notification Procedures

A PII Controller that has experienced a Security Breach of Category I PII shall provide Notice of the Security Breach to any PII Subject associated with the PII in question unless the PII Controller determines following an analysis considering the factors set out in Section B above, and maintains such determination notwithstanding any new information obtained by the PII Controller subsequent to conducting such an investigation, that the Security Breach is unlikely to have caused and is unlikely to cause Harm to that particular PII Subject.

If a PII Controller that has experienced a Security Breach of Category II PII determines following an investigation conducted in accordance with Section B above, or based upon new information obtained by the PII Controller subsequent to conducting such an investigation, that the Security Breach likely caused or is likely to cause Harm to one or more of the PII Subjects associated with the PII in question, then the PII Controller shall provide Notice of the Security Breach to each PII Subject as to which the PII Controller made such determination.

Where an obligation to provide Notice of a Security Breach to a PII Subject exists under this Paragraph D, such Notice shall be provided either by the PII Controller or by another party that has an agreement with the PII Controller that allows the PII Controller to require the other party to provide such Notice absent exigent circumstances. The PII Controller remains responsible for ensuring that Notice of the Security Breach is provided, either by itself or by its service provider or contract partner.

Where an obligation exists under this Paragraph D above to provide Notice of a Security Breach to a PII Subject, such Notice to such PII Subject should be provided either through traditional U.S. mail or, if the party providing the notice has previously communicated with the PII subject via email, through email with a subject line that will ensure that the message 1) will

be delivered to the PII Subject and will not be captured by spam or junk filters; 2) will communicate the importance of the notice; and 3) will encourage the PII Subject to read the notice.

If the PII Controller does not have access to the U.S. mail or email of each PII Subject, the PII Controller shall make a post for at least 60 days on the PII Controller's website if the PII Controller maintains one. This post shall consist of a link to the Notice on the home page or first significant page after entering the website that is in larger or contrasting type, font, or color to surrounding text of the same size or set off from other text by symbols or marks that call attention to the link. If the PII Controller does not have a website, notice may be given through notification to major print or broadcast media where the affected individuals likely reside.

PII Controllers shall provide supplemental Notice to individuals as reasonably needed, as new information about a breach is uncovered through the course of investigation, including but not limited to new information about the nature of the breach or the individuals affected, or if new information informs a PII Controller that the Security Breach likely caused or is likely to cause Harm. Supplemental Notice should be made in the same manner as the original notices.

E. Form of Notice

Any Notice required to be given to a PII Subject by Paragraph D shall be in the following form and shall include at least the following information:

- Title "NOTICE OF DATA BREACH" in all capital letters
- Salutation: "Dear [First and Last Name of Individual]:"
- Introductory Statement:
    a. Brief statement of why the Notice is being sent to the PII Subject.

b. For example: "We are writing to provide you with information about a data incident involving [Name of organization experiencing the breach]. You are receiving this letter because you [Describe relationship between the PII Subject in question and the PII Controller in question]."

- What Happened?
  a. Brief description of the Security Breach that triggered the notification, including the number of individuals involved, if known.
  b. Date of Security Breach discovery and, if known, date range during which the Security Breach occurred.
- What Information Was Involved?
  a. Description of the PII in question specific to the PII Subject.
- What Are We Doing About It?
  a. General description of any actions taken by the PII Controller to address the Security Breach.
  b. Who else has been notified? (Law enforcement, credit bureaus, state agencies)
  c. Describe cooperation with law enforcement, as appropriate.
- What Can You Do?
  a. General description of/recommendations for what the PII Subject can do to further protect himself/herself from whatever Harm the PII Controller has determined the Security Breach has likely caused or is likely to cause the PII Subject.

Where appropriate, the "What Can You Do" section may include any or all of the following:

i. Contact information for three major credit bureaus, and statement of right to free credit report;

ii. Contact information for FTC; and

iii. Contact information for State Attorney General/ Protection Agency

- Where required by Paragraph G, include offer of services called for by Paragraph G.
- For More Information: Provide contact information for point person at entity giving the Notice to respond to questions and/or address concerns that the PII Subject can use to inquire about the Security Breach and the other matters set forth in the Notice.

F. Notification Timeline

Where an obligation exists under Paragraph D to provide Notice of a Security Breach to a PII Subject, such Notice shall be provided without unreasonable delay and in an expedient manner but not later than 60 days after the PII Controller in question first came to believe, or reasonably should have come to believe, that a Security Breach had occurred as to the PII associated with such PII Subject, unless good cause exists to delay providing such Notice.

G. Identity Theft Prevention and Mitigation Services

Where an obligation exists under Paragraph D to provide Notice of a Security Breach, such Notice shall include an offer to provide credit monitoring in combination with identity theft prevention and mitigation/restoration services, all of which services shall be provided at no cost to the PII Subject in question, for not less than 24 months, along with all information necessary

to enable such PII Subject to take advantage of the offer, if the Security Breach in question involved unauthorized Access to the PII Subject's Social Security number, driver's license number, or state or federal identification number (e.g., passport number). For purposes of the preceding sentence, "identity theft mitigation and restoration services" shall include, but are not necessarily limited to: (1) assistance with communicating with creditors and debt collectors; (2) notifying lenders and credit card companies; (3) providing information and assistance with notifying state's Department of Motor Vehicles in connection with driver's license fraud, notifying the FTC and the Social Security Administration for Social Security number fraud, the U.S. State Department, Passport Services Department for passport fraud, and the U.S. Postal Service for mail theft; (4) dark web monitoring; or (5) assistance to the PII Subject in question in placing a freeze on his or her credit report to prevent an identity thief from opening new accounts in his or her name, and in completing the necessary forms. The PII Subject shall not be charged for any of these services, nor shall the PII Subject be "upsold" any services in connection with these services. The PII Subject shall receive notification before any such services described in this section expire, and in no event shall the PII Subject be automatically charged for a continuation of such services after they expire unless the PII Subject explicitly elects to continue such services via separate communication and in writing.

H. Regulator Notification

Where an obligation exists under Paragraph D above to provide Notice of a Security Breach to a PII Subject, Notice of such Security Breach shall simultaneously be provided to [enacting authority to identify Notice recipient], in the form and manner specified by such entity. Notwithstanding anything to the contrary in the preceding sentence, in the event Notice of a particular Security Breach is required to be given to multiple

governmental entities within a state or to multiple jurisdictions, the Notice required by the preceding sentence may be provided via centralized reporting through [insert website], in the form and manner specified by such website, with such Notice to be processed and forwarded to government entities as specified by such website.

COMMENTARY ON U.S. SANCTIONS-RELATED RISKS FOR RANSOMWARE PAYMENTS

A Project of The Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

Author:

The Sedona Conference

Editor-in-Chief:

Jim Shook

Contributing Editors:

John Gray
Eric B. Gyasi
Bill Hardin
Emily Jennings
Robert Kirtley
Jon Polenberg
Daniel E. Raymond
W. Lawrence Wescott
Zachary Willenbrink
Philip N. Yannella

Steering Committee Liaison

Alfred J. Saikali

Staff Editors:

David Lumia
Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 11. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of

the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

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.

This publication may be cited as follows:

> The Sedona Conference, *Commentary on U.S. Sanctions-Related Risks for Ransomware Payments*, 25 SEDONA CONF. J. 617 (forthcoming 2024).

PREFACE

Welcome to the October 2024 final version of The Sedona Conference's *Commentary on U.S. Sanctions-Related Risks for Ransomware Payments* ("*Commentary*"), a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). 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 through dialogue and consensus.

The mission of WG11 is to identify and comment on trends in data security and privacy law, in an effort to help organizations prepare for and respond to data breaches, and to assist attorneys and judicial officers in resolving questions of legal liability and damages.

The Sedona Conference acknowledges Editor-in-Chief Jim Shook for his leadership and commitment to the project. We also thank contributing editors John Gray, Eric Gyasi, Bill Hardin, Emily Jennings, Robert Kirtley, Jon Polenberg, Daniel Raymond, Larry Wescott, Zach Willenbrink, and Phil Yannella for their efforts. We also thank Al Saikali for his contributions as Steering Committee liaison to the project and Guillermo Christensen for his contributions.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG11 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 WG11 annual and midyear meetings

where drafts of the *Commentary* were the subject of the dialogue. The publication was also subject to a period of public comment. On behalf of The Sedona Conference, I thank all of them for their contributions.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, patent litigation, patent remedies and damages, trade secrets, and artificial intelligence. 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
Executive Director
The Sedona Conference
October 2024

TABLE OF CONTENTS

I. INTRODUCTION

Threat actors, using ransomware attacks,[1] are preying on computer networks of organizations worldwide. Utilizing malware and other tools, threat actors encrypt both data and applications and prevent access to an organization's cyber network, causing an abrupt stop to, material disruption of, or significant degradation in an organization's ability to conduct business. These threat actors demand a ransomware payment in return for a decryption tool used to regain network access and increasingly also attempt to extort ransomware victims by threatening to publicize stolen data. Ransomware attacks can result in substantial costs, serious disruptions to essential services and supply chains, and even risks to life. Determining whether to pay a ransom or work to recover systems without access to the decryption tool is a difficult and often expensive decision.

In the United States, no federal laws[2] have been enacted specifically to limit the payment of cyber ransoms.[3] However, the U.S. Treasury's Office of Foreign Assets Control (OFAC) has explained that such payments may subject ransomware victims to liability under the Trading With The Enemy Act (TWEA) and/or the International Emergency Economic Powers Act (IEEPA). Generally, those laws prohibit U.S. persons from transacting or

1. "Ransomware attack" means the deployment of malicious software for the purpose of demanding payment in exchange for restoring critical access to, or the critical functionality of, an information and communications system or network.

2. Some state laws restrict the ability of certain organizations to pay cyber ransoms. *See, e.g.*, FLA. STAT. 282 § 3186(2022).

3. The U.S. federal government has imposed rules for certain organizations, primarily those dealing with critical infrastructure, to report ransomware payments. In addition, money laundering laws require entities involved in the processing of ransomware payments to file disclosures through Suspicious Activity Reports that are submitted to the U.S. Department of Treasury's Financial Crimes Enforcement Network.

attempting to transact with an enemy of the U.S., certain related parties, and specified parties subject to U.S. sanctions or embargoes.

OFAC has published two advisories in recent years on the subject of ransomware payments, both of which suggest that U.S. persons may be held strictly liable under TWEA and IEEPA when they make a ransomware payment to a sanctioned person or engage with an embargoed country or region.[4] Strict liability in this context means that any U.S. person may face a civil enforcement action by OFAC for transacting or attempting to transact with an enemy of the U.S. even if the person did not know or have reason to know that a ransomware payment was being made to a sanctioned person or embargoed country or region.[5]

Contrary to OFAC's advisories, TWEA and IEEPA and their regulations do not impose a strict-liability standard in all cases where a victim makes a ransomware payment to a threat actor on the Specially Designated Nationals and Blocked Persons list ("SDN List"). However, OFAC's interpretation of these statutes and regulations as imposing a strict-liability regime creates substantial uncertainty and unnecessary chilling effects when victims are forced to make ransomware payments. It is often difficult to identify the recipient of a ransomware payment before making it, leaving ransomware victims uncertain about whether

4. *See* U.S. DEP'T OF TREASURY, ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS (Oct. 1, 2020), *available at* https://ofac.treasury.gov/media/48301/download?inline [hereinafter OFAC 2020 GUIDELINES] and UPDATED ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS (Sept. 21, 2021), *available at* https://ofac.treasury.gov/media/912981/download?inline [hereinafter OFAC 2021 GUIDELINES].

5. Willful or intentional violations of TWEA, IEEPA, or the associated regulations may also result in criminal enforcement by the U.S. Department of Justice.

payment is to a sanctioned person or an embargoed country or region. Additionally, given the federated nature of threat actors and how threat actors align with larger threat groups, it may be very difficult to determine if a payment will be received by a threat actor or group that contains a sanctioned person. Finally, in many scenarios—like those involving risk of physical harm or large-scale economic disruptions—making a ransomware payment could prevent substantial harm. When factors weigh in favor of making the ransomware payment, imposing strict liability is both bad policy and bad law for a ransomware victim, who has no reason to know (and importantly, no time to determine) that the recipient is a sanctioned person or in an embargoed country or region.

This *Commentary* reviews these issues in three parts:

Part 1

An analysis of TWEA and IEEPA; OFAC's recent guidance; and the purported strict-liability standard;

Part 2

A Framework for assisting organizations in identifying the source of an attack and likely recipient of a ransom and evaluating organizations' level of risk from OFAC if the organizations elect to pay; and

Part 3

Suggestions for a more reasoned basis for determining circumstances under which a ransomware payment might be made without the threat of OFAC sanctions.

II. CURRENT LEGAL FRAMEWORK

A. Background

TWEA and IEEPA generally prohibit U.S. persons from transacting or attempting to transact with an enemy of the U.S., certain related parties, and any person, country, or region that is subject to a U.S. sanctions order or embargo ("Sanctioned Parties"). OFAC is responsible for civil enforcement of these laws, issuing related regulations, and maintaining the SDN List, which identifies Sanctioned Parties. According to OFAC, it "administers and enforces [these] economic sanctions programs primarily against countries and groups of individuals, such as terrorists and narcotics traffickers. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals."

Currently, there is no OFAC sanctions program that applies to all ransomware threat actors. Instead, the relevant sanctions primarily affect specific actors who are connected to sanctioned or embargoed nation-states (for example, Evil Corp and Lazarus, which are connected to Russia and North Korea, respectively) and, more recently, certain exchanges for cryptocurrency that have been used by ransomware threat actors to transfer funds. For example, on the SDN List, OFAC has designated the names of individuals known to be affiliated with a particular threat actor (such as Evil Corp) or the name given to their malware (such as Dridex or TrikBot). OFAC has also identified digital wallet addresses used by certain threat actors.

In other words, OFAC's approach to designating threat actors relies on the identity of the Sanctioned Parties. Thus, to determine whether a threat actor is a Sanctioned Party, a ransomware victim must attempt to attribute the attack to an identifiable person or group.

However, as ransomware schemes have proliferated in recent years, and with more attention being paid to sanctioned-party risks, ransomware victims, incident responders, and their legal counsel have faced increasing challenges in trying to determine whether a threat actor is a Sanctioned Party or is affiliated with a Sanctioned Party—a process commonly known as "attribution." Attribution is particularly difficult in the context of cybersecurity threat actors who engage in criminal activity, sometimes act on behalf of (or with the tacit approval of) nation-states; license malware from criminal developers; and generally take extensive measures to obfuscate their identities and activities. Attribution may also take longer than the time allowed by a threat actor for a ransomware payment—i.e., even when the cybersecurity threat actor may be identified, such identification may occur months or years after the immediate incident or the deadline for a ransomware demand.

B. Current OFAC Guidance

There is no published case law that directly addresses OFAC sanctions or enforcement in the ransomware context.[6] OFAC has issued two advisories focused on ransomware[7] (in 2020 and 2021), but those advisories provide little guidance on identifying Sanctioned Parties. Ransomware victims (and the various third parties involved in responding to ransomware incidents)

---

6. In similar contexts involving extortion by Sanctioned Parties, enforcement actions have been brought against parties making payments to the extortionists. *See, e.g.*, Press Release, U.S. Dep't of Justice, Chiquita Brands International Pleads Guilty to Making Payments to a Designated Terrorist Organization And Agrees to Pay $25 Million Fine (Mar. 19, 2007), *available at* https://www.justice.gov/archive/opa/pr/2007/March/07_nsd_161.html#:~:text=Chiquita%27s%20Payments%20to%20the%20AUC&text=Chiquita%2C%20through%20Banadex%2C%20paid%20the,a%20senior%20executive%20of%20Banadex.

7. *See* OFAC 2020 Guidelines and OFAC 2021 Guidelines, *supra* note 4.

therefore face significant uncertainty in trying to determine whether a threat actor is a Sanctioned Party and, in turn, whether a ransomware payment (or their facilitation of such a payment) might be unlawful.

The OFAC advisories identify the risk that ransomware victims and incident responders face from the potential application of a strict-liability standard. Specifically, both advisories[8] explain:

> OFAC may impose civil penalties[9] for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.

In addition, OFAC's Economic Sanctions Enforcement Guidelines[10] identify knowledge and intent factors that will be considered in determining the proper enforcement mechanism in a given case, suggesting that those factors may be relevant only after a liability determination has been made rather than in the liability determination itself.

Nonetheless, to date, there are no reported instances of OFAC bringing an enforcement action against a victim or third party for facilitating a ransomware payment. And OFAC has

---

8. *Id*.

9. The maximum civil penalty amount is adjusted for information by OFAC from time to time. In 2021, the maximum civil penalty amount was the greater of $311,562 or twice the amount of the prohibited transaction. Inflation Adjustment of Civil Monetary Penalties, 86 Fed. Reg. 14,534 (Mar. 17, 2021), *available at* www.federalregister.gov/documents/2021/03/17/2021-05506/inflation-adjustment-of-civil-monetary-penalties.

10. 31 C.F.R. Part 501, App'x A.

not provided any additional clarity regarding its two ransomware advisories. There are, for instance, no FAQs that address issues and questions relating to those advisories, in contrast to the FAQs published by OFAC relating to sanctions against Russia, Iran, and North Korea.[11]

C. When Does Strict Liability Apply?

Despite OFAC's recent advisories and its enforcement guidelines, at least some of the provisions and associated regulations of TWEA and IEEPA do not impose strict liability. For example, multiple provisions of TWEA only prohibit conduct undertaken with "knowledge or reasonable cause to believe" that a counterparty is a foreign enemy or is acting on behalf of such an enemy.[12] Likewise, although certain regulations under IEEPA may impose strict liability,[13] at least some of its provisions and regulations require knowledge or willfulness to establish liability.[14] Ransomware victims and incident responders should therefore be aware that strict liability does not apply in

---

11. *See, e.g.*, *Ukraine -/Russia-related Sanctions*, U.S. DEP'T OF TREASURY - OFFICE OF FOREIGN ASSETS CONTROL, https://ofac.treasury.gov/faqs/topic/1576 (last accessed Oct. 16, 2024).

12. *See, e.g.*, 50 U.S.C. § 4303(a)-(b).

13. *See, e.g.*, 31 C.F.R. § 510.201(a)(1) ("All property and interests in property that are in the United States, that come within the United States, or that are or come within the possession or control of any U.S. person of the Government of North Korea or the Workers'' Party of Korea are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in.").

14. *See, e.g.*, 50 U.S.C. §§ 1705(c) (requiring willful violation to establish criminal liability), 1708(b)(2) (limiting application of section to foreign persons that the President determines "knowingly" engages in subject conduct), 1708(b)(4) (incorporating penalties from section 1705, including criminal penalties for "willful" violations), and 1708(d)(4) (defining "knowingly" for purposes of section addressing economic or industrial espionage in cyberspace).

all cases where a ransomware payment is made to a Sanctioned Party.

1. Legal Standards under TWEA

TWEA makes it unlawful:

> (a) For any person in the United States, except with the license of the President . . . to trade, or attempt to trade, either directly or indirectly, with, to, or from, or for, or on account of, or on behalf of, or for the benefit of, any other person, ***with knowledge or reasonable cause to believe*** that such other person is an enemy or ally of enemy, or is conducting or taking part in such trade, directly or indirectly, for, or on account of, or on behalf of, or for the benefit of, an enemy or ally of enemy.
>
> (b) For any person, except with the license of the President, to transport or attempt to transport into or from the United States, or for any owner, master, or other person in charge of a vessel of American registry to transport or attempt to transport from any place to any other place, any subject or citizen of an enemy or ally of enemy nation, ***with knowledge or reasonable cause to believe*** that the person transported or attempted to be transported is such subject or citizen.
>
> (c) For any person (other than a person in the service of the United States Government or of the Government of any nation, except that of an enemy or ally of enemy nation, and other than such persons or classes of persons as may be exempted hereunder by the President or by such person as he may direct), to send, or take out of, or bring into, or attempt to send, or take out of, or bring

> into the United States, any letter or other writing or tangible form of communication, except in the regular course of the mail; and it shall be unlawful for any person to send, take, or transmit, or attempt to send, take, or transmit out of the United States, any letter or other writing, book, map, plan, or other paper, picture, or any telegram, cablegram, or wireless message, or other form of communication ***intended for or to be delivered, directly or indirectly, to an enemy or ally of enemy***: Provided, however, That any person may send, take, or transmit out of the United States anything herein forbidden if he shall first submit the same to the President, or to such officer as the President may direct, and shall obtain the license or consent of the President, under such rules and regulations, and with such exemptions, as shall be prescribed by the President.[15]

In other contexts, similar legal standards have been construed to impose liability only when a person has actual knowledge of the relevant facts or acts in "deliberate ignorance" or "reckless disregard" of those facts.[16]

---

15. 50 U.S.C. § 4303(a)-(c) (emphasis added). Arguably, 50 U.S.C. § 4303(c) prohibits the cross-border communication of ***any*** "letter or other writing or tangible form of communication" in any other way than "in the regular course of mail," regardless of intent or knowledge as to the source or recipient of the communication. *See* Welsh v. U.S., 267 F. 819, 821 (2d Cir. 1920) (explaining that § 4303 creates two offenses, the first of which does not require any intent that the cross-border communication come from or be directed to a foreign enemy). That section, however, does not appear to have been enforced since the 1920s; it would seem to prohibit significant swaths of modern international commerce, and it might well be unconstitutional.

16. *See, e.g.*, 13 C.F.R. § 142.6 (in the context of Small Business Administration loans, a person knows or has reason to know that a claim or statement

2. Legal Standards under IEEPA

Separately, the penalty provision of IEEPA makes it "unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under [50 U.S.C. §§ 1701-1708]" and authorizes imposition of civil penalties for any such unlawful act.[17] Standing alone, that provision does not specify the level of knowledge or intent (if any) that must be shown before civil liability may be imposed but instead leaves that question to the language of the particular license, order, regulation, or prohibition at issue.[18] And many of the licenses, orders, regulations, and orders issued pursuant to IEEPA appear to impose strict liability in the sense that they do not have a specific mens rea or scienter requirement.[19] However, the specific provision of IEEPA relating to "economic or industrial espionage in cyberspace" only applies to conduct involving a foreign person "the President determines ***knowingly*** requests, engages in, supports, facilitates, or benefits from the significant appropriation, through economic or

---

is false if the person: "(i) Has actual knowledge that the claim or statement is false, fictitious, or fraudulent; or (ii) Acts in deliberate ignorance of the truth or falsity of the claim or statement; or (iii) Acts in reckless disregard of the truth or falsity of the claim or statement."); *see also* U.S. v. Heredia, 483 F.3d 913, 918, n.4 (9th Cir. 2007) (en banc) ("As our cases have recognized, deliberate ignorance, otherwise known as willful blindness, is categorically different from negligence or recklessness . . . . A willfully blind defendant is one who took deliberate actions to avoid confirming suspicions of criminality. A reckless defendant is one who merely knew of a substantial and unjustifiable risk that his conduct was criminal; a negligent defendant is one who should have had similar suspicions but, in fact, did not.").

17. *See* 50 U.S.C. § 1705(a).

18. *See In re* Criminal Complaint, Case No. 22-mj-067-ZMF, 2022 WL 1573361, at *2 (D.D.C. May 13, 2022) (Faruqui, M.J., mem. op.) (explaining that civil penalties may be imposed under IEEPA "on a strict liability basis").

19. *See, e.g.*, Exec. Order No. 14,065, 87 Fed. Reg. 10,293-96 (Feb. 21, 2022).

industrial espionage in cyberspace, of technologies or proprietary information developed by United States persons."[20]

Moreover, the licenses, regulations, orders, and prohibitions issued pursuant to IEEPA do not, in the aggregate, necessarily prohibit every possible transaction with every person or entity on the SDN List. Instead, those licenses, regulations, orders, and prohibitions are typically issued in connection with a specific conflict, series of events, or set of circumstances relating to a particular country, region, or group.[21] As a result, certain transactions with certain persons or entities on the SDN List would not violate any license, order, regulation, or prohibition issued under IEEPA and thus could not be penalized under 50 U.S.C.

---

20. 50 U.S.C. § 1708(b)(2) (emphasis added); *see also id.* § 1708(d)(4) ("The term ''knowingly,'' with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or should have known, of the conduct, the circumstance, or the result.").

21. For example, Executive Order 14,065 (recently issued in connection with the Ukraine-Russia conflict) prohibits, among other things:

- new investment in the so-called Donetsk People's Republic [DNR] or Luhansk People's Republic [LNR] regions of Ukraine or [other "Covered Regions"] by a United States person, wherever located;
- the importation into the United States, directly or indirectly, of any goods, services, or technology from the Covered Regions;
- the exportation, re-exportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, services, or technology to the Covered Regions; and
- any approval, financing, facilitation, or guarantee by a United States person, wherever located, of a transaction by a foreign person where the transaction by that foreign person would be prohibited by this section if performed by a United States person or within the United States.

See Exec. Order No. 14,065, *supra* note 19; *see also* 31 C.F.R. §§ 501-598 and Appendix.

§ 1705(a). Instead, these transactions could be penalized (if at all) only under TWEA, which, as discussed above, by its own express terms does not impose strict liability.

Further, several regulations issued under IEEPA include affirmative defenses or safe harbors relating to the knowledge or intent of the alleged violator.[22] For example, a transfer that would otherwise violate OFAC's Cyber-Related Sanctions Regulations will not be deemed null and void if the alleged violator establishes "to the satisfaction of OFAC" each of the following:

1. Such transfer did not represent a ***willful*** violation of the provisions of this part by the person with whom such property is or was held or maintained (and as to such person only);
2. The person with whom such property is or was held or maintained did not have ***reasonable cause to know or suspect***, in view of all the facts and circumstances known or available to such person, that such transfer required a license or authorization issued pursuant to this part and was not so licensed or authorized . . . ; and
3. The person with whom such property is or was held or maintained filed with OFAC a report setting forth in full the circumstances relating to such transfer promptly upon discovery that:
    i. Such transfer was in violation of the provisions of this part or any regulation, ruling, instruction, license, or other directive or authorization issued pursuant to this part;
    ii. Such transfer was not licensed or authorized by OFAC; or

22. *See, e.g.*, 31 C.F.R. §§ 578.202(d), 589.210(d).

iii. If a license did purport to cover the transfer, such license had been obtained by misrepresentation of a third party or withholding of material facts or was otherwise fraudulently obtained.[23]

In addition, some regulations issued under IEEPA negate strict liability by the language of the prohibition itself.[24]

3. Strict Liability Does Not Apply to All Ransomware Payments to Sanctioned Parties

In light of the foregoing, OFAC's advisories and enforcement guidelines—suggesting that any transaction of any kind with any actor on the SDN List automatically gives rise to strict liability—do not comport with the nuanced text of TWEA, IEEPA, and the associated regulations.[25] Some such payments create strict liability for penalties under IEEPA, but only where they violate a license, order, regulation, or prohibition issued under IEEPA that itself imposes strict liability. Otherwise, such transactions create no strict liability for penalties under either TWEA or IEEPA.

---

23. 31 C.F.R. § 578.202(d) (emphasis added). However, the filing of a report under 31 C.F.R. § 578.202(d)(3) "shall not be deemed evidence that the terms of paragraphs (d)(1) and (2) of [that] section have been satisfied." *Id.* § 578.202(e).

24. *See* Epsilon Elecs., Inc. v. U.S. Dep't of the Treasury, Office of Foreign Assets Control, 857 F.3d 913 (D.C. Cir. 2017) (explaining that 31 C.F.R. § 560.204—which prohibits, among other things, the exportation of goods to a third country that the exporter knows or has "reason to know" are specifically intended for re-exportation to Iran—does not include a strict-liability standard, and OFAC did not argue otherwise).

25. Arguably, OFAC's advisories are accurate to the extent they only reflect that OFAC ***may*** be able to impose strict liability in some cases. Many ransomware victims and incident responders, however, have construed the advisories to mean that OFAC believes strict liability applies in all cases involving ransomware payments to a threat actor on the SDN List.

Courts may give deference to OFAC's interpretation of its own regulations, including potential deference to the statements regarding strict liability in its ransomware advisories.[26] But OFAC's advisories and enforcement guidelines interpret TWEA and IEEPA themselves, and those interpretations should receive no deference.[27]

Accordingly, in attempting to assess the risks and lawfulness of a potential ransomware payment, ransomware victims and incident responders should be aware that strict liability does not always apply.

D. Is OFAC's Licensing Option Feasible in the Ransomware Context?

OFAC has a licensing process that theoretically could be used in the ransomware context and that OFAC suggests is an option in its advisories. OFAC offers two types of licenses: general and specific. General licenses are not specific to the applicant but, instead, authorize a particular type of transaction for a class of persons without the need to apply for a specific license. There are no general licenses that currently apply to ransomware payments.

A specific license is a written document issued by OFAC to a particular person or entity authorizing a transaction in

---

26. *See* Kisor v. Wilkie, 588 U.S. 558, 576 (2019) (even nonbinding interpretations of agency's own regulations may be given deference under *Auer v. Robbins*, 519 U.S. 452 (1997)).

27. *See* Loper Bright Enterprises v. Raimondo, 603 U.S. —, 144 S.Ct. 2244 (2024) (*overruling* Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837 (1984)); *see also* Christensen v. Harris Cty., 529 U.S. 576, 587 (2000) (unlike an agency's interpretations of its own regulations, its informal interpretations of statutes, "like [those] contained in policy statements, agency manuals, and enforcement guidelines, all of which lack the force of law" did not receive deference even under *Chevron*).

response to a license application. The specific license application process involves an application that can be submitted on OFAC's website. Typically, a license applicant should include as much detail about a transaction as possible, including the purpose of the license, the names and contact information of all parties involved, and as much documentation as possible.

There is no timeline for OFAC to issue a decision on a license request. OFAC warns that the length of time will vary depending on the complexity of the transaction(s) under consideration, the scope and detail of interagency coordination, and the volume of similar applications awaiting consideration. From collected prior experience, it may take OFAC several months to several years to respond to license requests (with simpler transactions on the lower end, which a ransomware payment is not). OFAC grants specific licenses on a case-by-case basis but noted in its September 2021 Advisory that OFAC will apply a presumption against granting specific licenses in the ransomware context.[28] Technically, it is possible to appeal a denial of a specific license as a "final agency action" in federal court under the Administrative Procedure Act. It is unlikely, however, that such an appeal will be successful given the current deference afforded OFAC by courts.

Practically speaking, victims and incident responders trying to use the licensing process in the ransomware payment context face major hurdles. First, the victim must know the ransomware payment is going to an individual SDN or otherwise implicates a sanctioned country, region, or government, but strong attribution to an SDN or sanctioned region in the beginning of a ransomware incident is difficult for the reasons described above. Certainly, the ransomware victim could submit an online application without providing much information. But there is no

28. OFAC 2021 Guidelines, *supra* note 4.

reason to ask for a license from OFAC if the ransomware victim does not know the transaction is prohibited by OFAC. Similarly, OFAC will not grant a specific license if the underlying transaction is not prohibited—in those situations, OFAC may provide a No License Required determination, which in itself can act as assurance that the conduct for which a license was sought does not fall within the category of prohibited activity. Therefore, submitting a license application without sufficient information is not likely to result in anything more than alerting OFAC of the issue before making a payment (which is not the purpose of seeking a specific license).

Second, assuming the ransomware victim has the information sufficient to complete the application, the victim needs to file an application for a specific license and receive a response from OFAC—granting the license—before making a payment. Most ransomware victims, however, are not in a position to wait months or years for OFAC's decision before making a payment; the act of delaying the payment pending a decision by OFAC on a license instead may function as a decision not to make the payment at all (especially given potential ransomware demand deadlines).

Third, and most compelling, OFAC has said there is a presumption against granting a license in the ransomware context. This presumption is a strong indication that OFAC is not willing to use the license process to resolve the sanctions issue faced by victims who decide they need to make a ransomware payment. It also means that a victim seeking an OFAC license may delay or decline to make a ransomware payment pending the outcome of OFAC's determination, only to have that license denied and the victim end up in the same situation it started with—forced to decide whether to make a ransomware payment without any understanding as to whether it's prohibited by OFAC or could subject itself to liability.

Absent a Freedom of Information Act request, there are no publicly available statistics tracking license applications, but the drafters' collective experience suggests that there have been very few, if any, licenses granted in connection with ransomware payments. For example, some insurers have sought licenses to reimburse ransomware victims, but it appears that no such licenses have been granted.[29]

In sum, due to the accelerated speed needed for a payment decision, the slow speed of the OFAC licensing process, and OFAC's reluctance to weigh in on attribution, the current license process is not a workable solution for ransomware victims, incident responders, or legal counsel concerned about OFAC enforcement.

E. OFAC's Approach Generates Uncertainty and a Chilling Effect

Despite scant enforcement activity in the ransomware context, OFAC's guidance and lack of a viable licensing option have affected incident responders in several ways:

- Most incident response companies have instituted some type of OFAC compliance check process, starting with rudimentary checks of digital wallets against the SDN List (a largely feckless process given that most threat actors create and dispose of wallets for each attack). Many of the OFAC compliance checks completed by incident responders or a ransomware victim's counsel rely on unreliable and unverifiable technical indicators, which are often

29. This is perhaps a scenario in which a license involving ransomware might make sense or would at least be feasible—i.e., a situation in which cyber insurance coverage may be available to a ransomware victim, but an SDN has been identified as the payee after the victim has already made the payment but before the insurer has reimbursed the victim.

difficult to assess precisely because threat actors obfuscate to avoid law enforcement and being placed on a no-pay list (if they were identified with an SDN/sanctioned country).

- Certain ransomware threat actors have been placed on no-pay lists by some incident responders for reasons related to OFAC's advisories. For example, some companies stopped payments to the Russian threat actor Conti when some reports linked its operators to Russian security services. In another instance, a threat actor advertised that it was shifting its hosting services to Iran, which immediately led to at least one incident response company banning payments to that threat actor. In response, the threat actor promptly issued a second press release walking back its plan to shift to Iran.
- The professionalization of ransomware-as-a-service (RaaS) platforms has further complicated the attribution for OFAC purposes. RaaS allows a segmentation of the cyberattack process. Broadly speaking, threat actors have specialized for-sale services for each of the four phases of a ransomware attack—access, network mapping, malware deployment, and ransomware detonation. This makes "attribution" that much more difficult given that different groups play different roles in different aspects of a ransomware attack.
- As part of the OFAC check, some incident response companies go so far as to ask the threat actors, during the payment negotiations, to identify themselves.

- Anecdotally, we also understand that some ransomware victims and incident responders prefer not to ask which threat actor is involved, under the mistaken theory that ignorance presents some defense or makes it more likely that cyber insurance will not be put at risk.
- Almost all insurance carriers offering cybersecurity coverage require some form of "sanctions" attestation before authorizing ransomware payments under a policy.[30]

Further, under OFAC's guidance, the implications for incident responders appear clear on the surface but are in fact problematic. On the one hand, the OFAC advisories appear to suggest that all entities involved in incident response—from legal counsel and forensic investigators to companies facilitating the transfer of cryptocurrency—can mitigate the risk from an unintentional dealing with an SDN or a threat actor in a sanctioned country. In theory, this can be done by instituting compliance checks and working with law enforcement. This is difficult to accomplish in reality for two reasons. First, most of the information likely to assist incident responders with attribution is in the hands of either the government (FBI, Secret Service) or some of the largest cybersecurity companies. Second, organizations must make a payment decision in an accelerated time frame that leaves very little time to determine the identity of a threat actor who is committed and has taken specific steps to mask its identity. This leaves OFAC's suggestions for mitigation without any practical means for implementation during an actual incident. More specifically, incident responders are left to rely upon their own experience with past clients, open-source/public reporting,

30. These attestations would likely do little to protect the carriers if OFAC applied a strict liability approach.

or, in limited instances, whatever information is available from law enforcement.

This haphazard approach incident responders are forced to undertake to identify a threat actor is in stark contrast to the kind of processes that businesses in the U.S. have implemented to comply with other OFAC requirements—e.g., collecting know-your-customer ("KYC") information on banking customers or registration/ownership documents for third parties, which can then be screened against the OFAC SDN List.[31]

A similar compliance approach to OFAC checks for ransomware is very difficult with respect to threat actors that operate in criminal forums and are often highly motivated and skilled in obfuscating their nationality or location. Moreover, OFAC itself provides no actionable information on how to identify an SDN in the ransomware context. Again, some of OFAC's ransomware-related designations involve identifying certain digital wallets associated with a handful of threat actors, but as noted above, such identification is largely meaningless, given the disposable nature of those wallets. And, to the extent that OFAC has designated a ransomware "group" by a moniker such as "Evil Corp," or by reference to a type of ransomware, such as Dridex, that is unhelpful because these groups are informal, constituted ad hoc, and often use specialists who may work across several groups or platforms.

In short, ransomware incident responders can rarely be sure whether a threat actor is a Sanctioned Party; thus, they can rarely be sure whether a ransomware payment is lawful. As a result, many ransomware victims may choose not to make ransomware payments, even when doing so would have been

31. Despite being well established and generally effective, these KYC processes still fail frequently—due, for example, to incorrect spellings of names or other technical or human errors—and such failures can still lead to liability.

lawful (where the threat actors are not, in fact, Sanctioned Parties), and perhaps even when doing so would prevent substantial economic hardship and/or physical harm.

III. ASSESSING THE RISK OF MAKING A RANSOMWARE PAYMENT

A. Introduction

Regardless of whether strict liability or some other standard (such as "knowledge or reasonable cause to believe") applies, organizations plainly face some level of sanctions-related risks in making ransomware payments. This section provides guidance on appropriate steps to assist in the attribution process and a discussion as to how the findings from that process, even if inconclusive, can inform the level of sanctions-related risk if a payment were to be made.

B. Attribution Process

The process of attributing the activities surrounding a ransomware attack to a given threat actor or crime syndicate is more art than science. The process outlined below cannot provide certainty that the hands on the keyboard are the threat actor; however, it provides a Framework for ransomware victims to evaluate risk.

The ransom note is the first line of identification. Threat actor notes are customized to their brand. For example, the ransom note created by Hive ransomware states that it is from the Hive threat actor group and provides information on a Tor Node with the group's leak site and a channel for communications. These notes are cataloged on many third-party sites and by law enforcement. Lastly, most threat actors have a leak site, maintained in the deep and dark web, where ransomware victims are directed.

After the ransom note has been provided, secondary indicators are used to complement the analysis. These indicators can include forensic findings such as the 1) encryptor used, 2) the internet protocol (IP) addresses used by the threat actor, 3) the attack kit, such as scanning tools, used by the threat actor, 4) the

manner in which data exfiltration was performed by the threat actor (if applicable), and 5) discussions with third-party sources such as law enforcement regarding any similar such attacks at other organizations.

The encryption tool, if recoverable, provides many clues on the coding of the malware. For example, Alpha Black Cat uses an encryptor built on the RUST platform. The encryption program will normally generate the ransom note after the tool is run during the attack. A properly equipped researcher can run the tool in a safe sandbox environment, which can help to understand the algorithms used and then use that information to connect to certain threat groups. This detailed investigation takes both trial and error, dedicated effort, and most importantly, time.

Once an agreement on payment is made with the threat actor, a cryptocurrency wallet identifier is provided, and that identifier may be another indicator to determine whether a Sanctioned Party appears to be the intended recipient of the funds. Although ransomware incidents typically involve unique, one-time-use wallets created specifically for each attack, some wallets have been tied to certain threat actors through forensic analysis, which can allow for subsequent identification, but usually well after the incident. Wallets can also be examined through several programs that provide intelligence about the wallet being used, the cryptocurrency exchange, and other potentially useful information.

Another approach is to combine sources of information, such as blockchain analysis, detections from the ransomware victim's network systems, and threat intelligence analysis and other research, to provide counsel and client with as much information as possible to make an informed decision as to whether a threat actor is a Sanctioned Party.

As above, blockchain analysis examines the cryptocurrency wallet provided by the threat actor. Cross-checks can be performed against the wallet itself, and any other wallets associated with it, as well as transactions against the wallet, against the Sanctioned Party, and other global watchlists. Various tools can provide insights on the threat actor's wallet, as well as other associated wallet addresses previously seen by the incident response firm. To underscore, these are usually retrospective due-diligence steps with limited utility during an incident where a threat actor uses a fresh wallet.

The ransomware victim's antimalware or endpoint detection and response system will contain indicators of compromise and/or malware signatures that can be compared against government repositories, other threat intelligence sources, or the incident response firm's own database of indicators of compromise. Other evidence will include the behavior of the malware within the environment, such as the method of infiltration and how the malware moved through the ransomware victim's environment, which can be matched against behavior patterns of other variants. Information can sometimes be gleaned from reverse-engineering the malware.

Other sources of intelligence include the incident response firm's security operations center, forensic vendors, and open-source intelligence—the dark web, or information from other security researchers. Cooperation with law enforcement is an important step that should be encouraged and has, on occasion, provided some valuable information.

If and once a payment is made, additional tracing of the wallet is generally not performed by the ransomware victim or incident responder. However, postpayment tracing may be undertaken by law enforcement, the Treasury Department's Financial Crimes Enforcement Network, and certain companies involved in monitoring crypto exchanges, who are building up

more granular tracing information. Another exception is when a threat actor re-ransoms a client for additional funds and provides a new wallet ID to the ransomware victim—in that instance, the original wallet ID would usually be reanalyzed.

C. Framework for Assessing Risk of Payment

The process of attributing a ransomware attack to a threat actor is complex, time-intensive, and has an uncertain outcome. Experienced forensic analysts who have handled hundreds of ransomware attacks may not be able to reliably attribute a ransomware attack to a particular threat actor. In fact, in many cases, a lack of reliable attribution is the assumed result.

The OFAC strict liability structure for payments to Sanctioned Parties thus gives rise to significant uncertainty for companies contemplating whether to make a ransomware payment. To help ransomware victims assess the degree of OFAC risk they may face for making a ransomware payment, this *Commentary* proposes a Framework. Due to the relative opacity of existing OFAC guidance, the lack of any OFAC sanctions to date against entities making payments to Sanctioned Parties, and a lack of judicial rulings, it is not possible to quantify the risk to an entity for making a prohibited payment. The proposed Framework instead serves as a methodology to enable entities to assess a level of risk of liability, as well as enforcement, based on the standards and guidance provided by federal regulatory authorities to date.

1. Framework Overview

The Framework involves consideration of two separate but related legal risks. First, the legal risk that a payment is actually sent to a Sanctioned Party, thus triggering strict liability under the OFAC regime; and second, whether mitigating factors exist to influence the level of OFAC's sanctions if it chooses to enforce

sanctions on an improper payment. There are different facts and variables informing an analysis of each question. The ultimate legal risk to an organization considering whether to make a payment involves consideration and balancing of both risks.

The Framework borrows elements of the risk assessment methodology often used by information security groups when evaluating, for example, the sufficiency of their control environments. The Framework seeks to define "inherent risk"—the risk of OFAC liability based on attribution efforts—and "residual risk," which is the bottom-line risk to an entity when considering inherent risk as well as mitigating factors.

The Framework adopts certain key principles:

- First, although strict liability may not apply in all situations, as described above, the Framework assumes that OFAC would likely seek to impose strict liability in any enforcement action.
- Second, under the strict-liability Framework, the reasonableness of the steps an entity takes to attribute a ransomware attack to a threat actor would have no bearing on whether a legal violation has occurred. The reasonableness of an organization's prebreach and postbreach actions, however, could be mitigating factors that would reduce the severity of any OFAC enforcement or imposed penalty.[32]

32. OFAC has identified the factors it considers in determining the nature and extent of any enforcement action. *See* 31 CFR Ch. V, pt. 501, App'x A. However, the drafters of this *Commentary* believe OFAC should provide additional clarification regarding its understanding of strict liability in this context and its application of mitigating factors.

- Third, in general, as confidence that a threat actor is a Sanctioned Party increases, inherent legal risk increases.

2. Applying the Framework

Hypothetical One

A large, sophisticated organization suffers a ransomware attack that significantly degrades its ability to timely process new online customer orders. The organization has completed regular employee training, maintains an information security plan that aligns with relevant regulatory and industry standards, and has a robust business continuity plan that is nonetheless unable to fully restore affected servers. The organization files an Internet Crime Complaint Center (IC3) report and remains in regular dialogue with the FBI concerning the event.[33]

The threat actors appear to be a new or unknown group, based on the contents of the ransom note. The organization retains specialized ransomware negotiators to assist in negotiating with the threat actor and assessing whether the threat actor is on the OFAC SDN List. By assessing indications of compromise, forensic analysts believe the malware signature points to one of four possible threat actor groups. The analysts do further blockchain analysis of the crypto wallet that the threat actors provide for facilitation of the ransomware payment. This analysis leads the experts to conclude that there is a significant probability that the threat actors are Iranian nationals.

33. The Internet Crime Complaint Center (IC3) is the FBI's standard portal for reporting cybercrime.

Risk Assessment

Attribution Steps	• Indications of compromise • Ransom note • Blockchain analysis • Threat intelligence
Confidence Level	Significant probability that actors are Iranian nationals
Inherent Risk	High
Mitigation Factors	• Incident Response Plan • Regular training • Business continuity program • Notification to and regular communications with federal authorities
Residual Risk	Medium-High

Analysis

This scenario involves a sophisticated organization that undertakes substantial efforts to attribute a ransomware attack. Those steps reveal a high likelihood that the threat actors are Sanctioned Parties or affiliated with Sanctioned Parties. Therefore, a ransomware payment to the threat actors would be in violation of OFAC sanctions, giving rise to a significant possibility of penalties based on OFAC's stated position.

However, the organization has also undertaken substantial preattack steps to prepare for, avoid, and remediate a ransomware attack. The organization also promptly notified federal authorities about the event and kept them regularly informed. These are mitigating factors that should lessen the likelihood of OFAC enforcement, and the organization could make a voluntary disclosure to OFAC itself, which might further reduce the risk of penalties.

Based on all of the foregoing, the residual legal risk of an OFAC penalty in this instance is medium-high, based on the high inherent risk.

Hypothetical Two

A small university lab suffers a ransomware attack that encrypts its research files, due to a phishing email. The university has not conducted any cybersecurity training for lab employees but uses multifactor authentication on relevant systems, pays for sophisticated antimalware software, and has a large IT department that enacts the university's incident response plan. The IT department is unable to restore the affected files, and the university files an IC3 report and responds in a timely fashion to additional questions from the FBI.

The threat actor identifies itself as a known group in the ransom note and is not on OFAC's SDN List. The university hires a ransomware specialist to further analyze the note and indications of compromise. The specialist finds that the attack is consistent with two other verified attacks by the self-identified threat actor. The specialist also conducts a blockchain analysis of the crypto wallet, which has been previously used, and concludes with a high degree of confidence that the wallet has been previously used by a threat actor not on the OFAC SDN List.

Risk Assessment

Attribution Steps	• Indications of compromise • Ransom note • Blockchain analysis • Threat intelligence
Confidence Level	High degree of confidence that actors are not on the SDN List
Inherent Risk	Low

Mitigation Factors	• Basic cyber hygiene practices • Incident Response Plan • Notification to and regular communications with federal authorities
Residual Risk	Low

Analysis

The ransomware victim is a small university lab that could have taken more preattack cyber hygiene steps to prevent the ransomware attack, such as regular employee training. Universities are an increasingly common target of ransomware attacks. However, the lab responds appropriately once the attack is made, and its attribution efforts reveal a low likelihood that the threat actors are on the OFAC SDN List. Therefore, a ransomware payment to the threat actors is unlikely to violate U.S. law or trigger any OFAC enforcement action.

Hypothetical Three

A medium-sized software development organization is the victim of a ransomware attack that results in the exfiltration of sensitive data and subsequent encryption of local file shares containing valuable customer data. The file shares had not been backed up.

Prior to the ransomware attack, the organization was in the process of building out its cybersecurity program but had been hampered by cost concerns and the recent departures of key employees from the Information Security department. The organization had not done cybersecurity training for employees in several years. In fact, the organization was surprised to learn that the data was even stored on local file shares, as its policies required storage of customer data in a secure cloud environment.

In response to the ransomware attack, the organization filed an IC3 report and reached out to local FBI agents, who provided

limited support and did not express significant interest in the attack. The organization also retained a forensic consultant. The consultant examined indications of compromise and other forensic artifacts, including the ransom note, and judged it more likely than not that the malware was not associated with any known threat actor groups, including any groups on the OFAC SDN List. Due to cost constraints, the organization declined to perform a blockchain analysis. The organization arranged payment to the threat actors and filed a Suspicious Activity Report (SAR) with the U.S. Treasury Department.

Risk Assessment

Attribution Steps	• Indications of compromise • Ransom note
Confidence Level	Moderate confidence that threat actors are not on SDN List, but this is based on truncated forensic analysis
Inherent Risk	Medium
Mitigation Factors	• Some cyber policies; immature cyber program • Violation of internal storage policies • IC3 report • FBI contact
Residual Risk	Medium

Analysis

This hypothetical involves incomplete attribution efforts that are arguably justified by virtue of the significant danger to the organization's business if a payment were not made to the threat actors, given the lack of backups. While there is no clear indication that the threat actors are on the SDN List, the organization could arguably have done more to confirm this assessment. The organization's prebreach mitigation efforts are,

likewise, less than complete. The organization's cyber program was immature, employee training was out of date, and there was a clear policy violation that led to the improper storage of customer files on local file shares that were not backed up. Post-breach mitigation efforts include filing of an IC3 report, outreach to the FBI (whose lack of interest may itself have been an indication that the threat actors were unlikely to have been on the SDN List), and the filing of an SAR. Overall risk in this scenario is medium, largely due to the lack of any forensic evidence of attribution to an entity on the SDN List and the FBI's apparent lack of concern. The overall risk, however, is not low because the organization's mitigation efforts were poor, and its attribution efforts could have gone further.

Hypothetical Four

A small dentist's office suffers a ransomware attack through a phishing campaign that affects access to a small volume of highly sensitive data: the Social Security numbers, financial information, and names of patients. The office previously conducted regular employee trainings on cyber hygiene but has not conducted any training since a change in management five years ago. The office uses antivirus software and believed that was sufficient to protect against cyberattacks. Employees searched for an incident response plan or policy but could not find one in the office's files. The office never renewed the cyber insurance policy that it carried up to five years ago prior to the management change, and no one at the office understands that an IC3 report should be filed. Several public postings have identified this threat actor as based in North Korea, based on a unique ransom note. The threat actor also identified itself as a North Korean group. The office pays the small ransom demand without consulting outside experts in an effort to avoid disruption to the practice and avoid giving notice to patients of the breach.

Risk Assessment

Attribution Steps	• Indications of compromise • Ransom note
Confidence Level	High probability that actors are North Korean nationals
Inherent Risk	High
Mitigation Factors	None
Residual Risk	High

Analysis

This scenario involves an unsophisticated business that undertakes no effort to attribute the ransomware attack or determine the legality of payment. The ransom note itself reveals a high likelihood that the threat actors are on the SDN List, although 100 percent attribution is not possible from a ransom note alone, given that threat actors are in the practice of obfuscation and deceit. Here, the ransomware payment to the threat actor is a clear violation of OFAC sanctions, giving rise to a significant possibility of penalties based on OFAC's stated position.

The business has undertaken minimal and outdated cyber hygiene steps and no postbreach mitigating actions, such as contacting law enforcement. In deciding not to consult an outside expert, office employees may have operated under the mistaken theory that ignorance would shield them from liability. The failure to notify patients of the breach presents additional risks beyond OFAC enforcement, including legal risks under state and federal data-protection and breach-notification laws.

The residual legal risk of an OFAC penalty in this instance is high, based on the high inherent risk, deliberate ignorance, and absence of mitigating factors.

IV. A PROPOSAL TO ADVANCE THE LAW: CREATION OF A SAFE HARBOR

A. Background

It is in the best interest of public policy that illegal and/or unauthorized cyber intrusions of all manner, scope, and scale are minimized or eradicated if possible. Paying ransoms to cyber threat actors is not a desirable outcome. OFAC summarized the situation thusly: "Such payments not only encourage and enrich malicious actors, but also perpetuate and incentivize additional attacks."[34]

That, however, is not the full extent of the story. This *Commentary* raises the question of whether preventing ransomware payments, based solely upon the presumed identity of the recipient of the funds, is a good or useful public policy. Arguments in favor of the public policy include: (a) fewer ransomware payments overall are likely to be made, based upon both prohibition when attribution can be made and the uncertainty generated when it cannot; (b) the most harmful nation-states and criminals, listed as Sanctioned Parties, should overall receive reduced funds from their criminal activities; and (c) with the reduced likelihood of ransomware payments, threat actors will be disincentivized from pursuing such activities.

Arguments against such a policy include, most prominently, the difficulty in determining the recipient of the funds, especially in the short timeframes necessary in ransomware scenarios. Section II(e), above, describes this difficulty in detail along with some of its consequences, including: (a) a chilling effect on advisors when they are most needed; (b) imposition of punishment for payments to Sanctioned Parties made by mistake; and (c) victims foregoing ransomware payments and incurring

34. OFAC 2021 Guidelines, *supra* note 4.

significant negative consequences on organizations, customers, clients, and other related third parties, even when such payments may have been legal, in the organizations' best interests, or have created significant and beneficial effects for third parties.[35]

In addition, there are situations where the benefits of making a ransomware payment might outweigh the costs and negative effects of paying a Sanctioned Party. For example:

- Healthcare: A hospital able to return to full operational capacity in hours or days, instead of weeks, reduces the risk of physical harm to patients who might not be able to receive proper treatment.
- Government Services: A water treatment or power-generating facility operating without proper safety controls or having to be shut down can endanger thousands of individuals.
- Economic: A large local or regional business that will suffer significant harm could endanger hundreds or thousands of jobs and the local economy.

Current guidance, however, does not specifically include consideration of these attack-specific circumstances. Accordingly, in keeping with The Sedona Conference's mission to move the law forward in a just and reasoned way, this *Commentary* identifies an alternative "safe-harbor" Framework that may offer a better path forward and be worthy of consideration.

---

35. *See, e.g.*, Jane Doe v. Lehigh Valley Health Network Inc., Case # 3:2023cv00585 (M.D. Pa. Apr. 6, 2023). The plaintiffs are patients whose nude healthcare photos were published by threat actors after the defendant refused to pay a ransom. https://dockets.justia.com/docket/pennsylvania/pamdce/3:2023cv00585/137513.

B. A Safe Harbor Framework

A "safe harbor" Framework may balance conflicting concerns. Generally, such a Framework would identify specific legal actions organizations can take to minimize or remove a specific legal liability that would otherwise attach in a given scenario.

In the ransomware payment scenario, this *Commentary* proposes that compliance with certain cybersecurity-related prerequisites could protect an organization from OFAC enforcement or otherwise reduce or eliminate OFAC-related liability for an organization making a ransomware payment to a Sanctioned Party. The discretion afforded to organizations who meet the prerequisites, we hope, would incentivize the voluntary adoption of better cybersecurity practices that immediately increase an organization's cybersecurity posture and, in the longer run, potentially lessen the severity of a cybersecurity attack if one occurred. This proposed safe harbor would not limit or eliminate any other liability in litigation or any federal, state, or administrative/regulatory proceeding. Nor, in the unfortunate event of a successful attack, would organizations that qualify for the safe harbor be required to pay a ransomware payment. It also would not immunize conduct in situations in which organizations know or have reason to know that they are facilitating payments to Sanctioned Parties. Organizations qualifying to make a ransomware payment may still ultimately elect to forego payment for a variety of reasons. In the best scenarios, such organizations will have undertaken sufficient preparation such that they do not obtain a substantial benefit from making a ransomware payment.

To be useful and successful, such a Framework must follow certain basic principles:

Principle 1: Minimum Security Standards. The safe harbor should only be available to organizations that

> **have implemented a minimum baseline of security controls and practices to reduce the overall risks of ransomware attacks and ransomware payments.**

The prerequisites necessary to qualify for the safe harbor can encompass various capabilities, which, if followed, should reduce overall risk and make ransomware attacks and payments less likely. Of course, attack methods and new technologies are constantly evolving, so the mandated controls and processes must be flexible enough to evolve with them. This *Commentary* has considered the sample factors and requirements set forth in Appendix A.

The *Commentary* acknowledges that, ideally, a ransomware safe-harbor qualification would address both the difficulties of attribution and balancing the potential harms to life, liberty, and the economic area or region (i.e., loss of jobs versus potential for facilitating a terrorist attack). Minimum security standards focus on the cyber hygiene of organizations prior to a cyber security attack. Increased cybersecurity posture helps to ensure that organizations are better positioned during the determination phase of attribution.

However, the *Commentary* maintains that minimum-security standards are nonetheless the best qualifier for the safe harbor in the context of ransomware payments. A balancing process is simply not practical. Most ransomware events include the possibility of harm to some individual or organization, and there is no practical method to weigh relative harm. Furthermore, in the compressed timeframe of a ransomware attack, entities may struggle to apply an imprecise, harm-based test. By contrast, as is discussed in greater detail below, it is significantly easier to make a "yes/no" determination of whether certain minimum-security standards have been met. Meanwhile, the upfront

capital costs and efforts that enhance cybersecurity and resilience should be encouraged and rewarded.

Principle 2: Clarity. The controls and practices required to qualify for the safe harbor should be sufficiently clear to permit organizations to quickly determine whether they qualify.

As discussed above, decisions regarding ransomware payments must be made quickly. Thus, for a safe harbor to be beneficial, organizations must be able to quickly determine whether they have qualified (better yet, they should be able to make this determination before an attack, if they have sufficient opportunity).

This means that any requirements must be reasonably specific. Sliding-scale requirements, such as those requiring organizations to adopt controls commensurate with their risk appetite, would reduce the usefulness of the safe harbor by preventing organizations from quickly determining whether they qualify. Therefore, efforts should be made to define the qualification requirements with the greatest specificity possible—perhaps, for instance, through identifying specific (but still adaptable) mandated controls and processes like those described in Appendix A.

The adoption of a preexisting framework, such as an NIST or ISO framework, for the safe harbor was considered but rejected. Such valuable but very detailed frameworks are sufficiently complex that organizations may struggle to determine whether they qualify for the safe harbor, thus defeating its purpose. Preferably, the safe harbor would identify a select number of controls and practices deemed most critical to resilient cybersecurity and identify specific thresholds applicable to organizations depending on their scale. However, a third-party certification of a cybersecurity standard such as ISO 27001 may be considered a superset of the controls required for the safe

harbor. As such, while they should not be required for safe harbor qualification, such certifications might be considered as automatic qualification.

Principle 3: Scaling Flexibility. The controls and practices required to qualify for the safe harbor should scale to account for organizational differences in sophistication, funding, personnel, and other real-world issues that often limit adoption of controls and processes, while setting minimum standards needed to mitigate and prevent as much facilitation of money to Sanctioned Parties as possible.

A safe harbor test should be flexible enough to recognize and account for organizational differences. To address these disparities while also maintaining simplicity and ease of use, easily determined categories—perhaps based upon an average annualized revenue or similar proxy for sophistication and budget capabilities—could be created along with requirements for controls and processes that scale to reflect what might reasonably be expected of organizations in each such category. Such a test should identify those processes that are most likely to assist organizations in preventing the transfer of funds to Sanctioned Parties so as to facilitate OFAC, foreign policy, and national security goals.

Principle 4: Technological Flexibility. The controls and practices required to qualify for the safe harbor should adapt to developments in technology, security, the law, and the threat landscape.

Cyber threats are constantly evolving, forcing the related technologies, security controls, and laws to keep pace (or at least *try* to keep pace). The safe-harbor qualifications, therefore, need to be flexible enough to adapt to changes quickly. Accordingly, to the extent that the safe-harbor qualifications are based upon

some third-party framework (*see* Principle 2: Clarity), it should be made clear that any applicable changes to that third-party framework are presumptively adopted into the safe-harbor qualifications. Similarly, if a regulator (either OFAC or another body) is responsible for creating the qualifications, then that regulator should also be: (1) required to routinely review the qualifications to evaluate whether changes are necessary; and (2) empowered to update the qualifications as quickly as possible.

Principle 5: Prepayment Notification. The safe harbor should require an organization to notify OFAC before making a payment.

Before receiving the benefit of the safe harbor, organizations should also be required to file a prepayment report with OFAC no later than 24 hours[36] before making the ransomware payment. The reporting regimen would be similar to the existing requirements for SARs. Filing a prepayment report would not relieve the payor from complying with any other provision of law.

The prepayment report should include a description of the ransomware attack, the ransomware payment demanded, and all other information concerning the ransomware attack obtained through good-faith efforts, including the party who committed the attack and demanded the payment (if known), and all other identifying information. Information about the ransomware payment should include the identity and verification of the hosted wallet[37] and the person who will engage in

36. A prepayment report should be updated upon any material change in circumstance or knowledge prior to payment being made. However, the update should not restart the 24-hour waiting period.

37. Hosted wallets are those for which a financial institution provides custody services for its customers'' convertible virtual currency.

transactions with unhosted[38] or otherwise covered wallet counterparties.

OFAC encourages victims and those assisting them with ransomware attacks to report the attacks and to contact OFAC if they suspect there may be a sanction connected to the ransomware payment. A safe harbor with a prepayment component would beneficially increase ransomware attack disclosure, providing the government with quick attribution information. Under the current framework, ransomware victims may choose to not report ransomware attacks at all or to delay their reports, rendering the information more remote and less useful.

38. Unhosted wallets are those that store private keys for convertible virtual currency in a software program or written records to conduct transactions privately rather than using the services provided by a financial institution.

V. CONCLUSION

OFAC's advisories and enforcement guidance suggest that a ransomware victim may be strictly liable whenever it makes a ransomware payment to a Sanctioned Party. Such strict liability does not apply in all circumstances, however, as the language of TWEA and IEEPA and the regulations thereunder make clear. OFAC's guidance regarding this issue creates a chilling effect on ransomware payments and may prevent ransomware payments that would be legal and would have positive net benefits. That guidance complicates matters not only for ransomware victims but also their incident responders, legal teams, negotiators, and insurers.

In the absence of further guidance or authority, ransomware victims may wish to utilize the risk-based Framework set forth above in attempting to attribute a ransomware attack and assess the potential liability resulting from a ransomware payment. However, OFAC and related policymakers should consider providing additional guidance and creating a safe harbor to encourage and enhance cybersecurity controls for all organizations.

APPENDIX A – SAMPLE FACTORS AND REQUIREMENTS FOR CONSIDERATION

Factor	Requirements
A. Governance	For all organizations, of any size: i. formal oversight by a qualified individual and/or board oversight; ii. written cybersecurity policies and procedures; iii. written incident response plan; and iv. annual certifications of compliance to a board or appropriate ownership group

Factor	Requirements
B. Technical Safeguards	For all organizations, of any size, multi-factor authentication for network access and email client access, along with password control protocols. The next level might add additional servers, endpoint detection and monitoring, and regular patching protocol. The highest-level organizations could be required to also implement: i. centralized firewall and security logging (with adequate retention period); ii. appropriate and reasonable network segmentation; iii. network and system monitoring; and iv. encryption in transit and at rest of any statutorily defined and protected class of personal information.

Factor	Requirements
C. Risk Assessments	For all organizations, of any size, annual penetration testing. The next level might add requirements to conduct: i. asset inventory; ii. data classification and criticality rating assessment; and iii. vulnerability scanning. The most sophisticated organizations would be required to conduct: i. cloud configuration assessments; ii. network assessments and mapping; and iii. annual vulnerability scanning.
D. Controls	All organizations, of any size, should conduct regular tabletop exercises. More sophisticated organizations should also: i. implement privilege access controls program; ii. ensure timely and effective data disposition; and iii. maintain audit trails and logs of data at rest, data in transit, and data in use.

Factor	Requirements
E. Postincident	All organizations would be required to notify appropriate law enforcement entities and extend cooperation to such law enforcement entities during any investigative process (e.g., sharing indicators of compromise).

COMMENTARY ON PROPORTIONALITY IN CROSS-BORDER DISCOVERY

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

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

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 6. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of

the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

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.

This publication may be cited as follows:

> The Sedona Conference, *Commentary on Proportionality in Cross-Border Discovery*, 25 SEDONA CONF. J. 669 (forthcoming 2024).

PREFACE

Welcome to the November 2024 final 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 also thank Nichole Sterling for her contributions as Steering Committee liaison to the project and 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. The publication was also

subject to a period of public comment. On behalf of The Sedona Conference, I thank both the membership and the public for all their contributions to the *Commentary*.

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, trade secrets, and artificial intelligence. 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
Executive Director
The Sedona Conference
November 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 discovery conflicts arising from compliance with non-U.S. laws are certainly not new, parties face a veritable storm of practical challenges and compliance burdens in cross-border discovery. This rising storm is due to a confluence of factors representing a new era in electronic information: the emergence of new and more stringent data protection laws; the evolution of existing data protection regimes; ever-increasing data volumes, formats, and complexity; 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

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).

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 potential 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. 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* courts should conduct a separate comity analysis. Applying these analytical steps in strict order should minimize analytic and doctrinal problems that can arise with common factors.

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 parties should make burden arguments with sufficient specificity 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.

3. 482 U.S. 522 (1987).

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 accelerated the generation and copying of large 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 word "proportional"

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

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] and adherence to local or varied data privacy and protection laws.[10] The Sedona Conference, like Rule 26, recognizes nonmonetary factors in determining discovery scope and has

---

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*].

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*].

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 are 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

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.

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 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

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.

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 also 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

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.

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]

Rule 34 required that a party seeking inspection or discovery of documents or tangible objects first shows 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 are neither new nor unique to 21st-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

20. *Id.* at 911.

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

22. Pike & Willis, *supra* note 17, at 301; Holtzoff, *supra* note 16, at 205.

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]

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

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.

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 the 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

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.

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]

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

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.

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*.

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

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

goal.[36] It also was clear that the intent was to include and give weight to 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]

---

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 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

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 Electronically Stored Information (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 effect 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

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.

perhaps most importantly, the amendments also moved the implicit proportionality factors outside the subsection defining the 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 overdiscovery 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,

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

> 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 and original place from the 1983 amendments. The "reasonably calculated" language was also removed, as it had been 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 resolving discovery disputes"—a responsibility that for 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. 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 ESI, coupled with rising data privacy and protection scrutiny, and the continued frustration of courts with the failure of parties to adhere to the spirit of the

42. No. 14 Civ. 9792 (WHP) (JCF), 2015 WL 7871037 (S.D.N.Y. Dec. 3, 2015).

43. *Id*. at *2–4.

amendments to the Rules[44] and The Sedona Conference's Principles of Proportionality by 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 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

---

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 electronic discovery 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).

"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 fewer documents 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. attorneys 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

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 Nov. 19, 2024); RONALD J. HEDGES, BARBARA JACOBS ROTHSTEIN & ELIZABETH C. WIGGINS, MANAGING DISCOVERY OF ELECTRONIC INFORMATION (3d ed. 2017), available at https://www.fjc.gov/content/323370/managing-discovery-electronic-information-third-edition.

than ever before—not just corporate defendants responding to discovery requests. Social media, mobile phone applications, collaboration software, and the move to cloud computing have 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.

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.

---

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 follow Nichols's request that Noom be ordered to either use a forensic application or create a program to collect hyperlinks from responsive documents when those hyperlinks may or may not have been relevant themselves. The court stated that it "is clear to this Court that there was no meeting of the minds on whether hyperlinks were attachments and this Court, when entering the order, did not view hyperlinks to be attachments." Nichols v. Noom Inc., No. 20-CV-3677 (LGS) (KHP), 2021 WL 948646, at *1 (S.D.N.Y. Mar. 11, 2021). The court engaged in a robust proportionality analysis to determine resolution of the hyperlinks dispute and noted that in "this Court's experience, only a fraction of the documents produced in discovery will be material to the litigation" *Id.*

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 not have 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

---

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

50. *Id.* at 195.

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]

---

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 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.

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

---

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.

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 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

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://www.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.

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).

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 the 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;
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;

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 Nov. 19, 2024).

> 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] Several factors 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;

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

67. *Id.* art. 7.

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

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 the processing of personal data to what is relevant and strictly necessary and by erasing unnecessary material without preserving it.[71] In the context of electronic discovery, 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]

---

69. *See* GDPR Recital 47, PRIVAZYPLAN, https://www.privacy-regulation.eu/en/r47.htm (last visited Nov. 19, 2024).

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 Nov. 19, 2024).

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

72. GDPR Recital 10, PRIVAZYPLAN, https://www.privacy-regulation.eu/en/recital-10-GDPR.htm (last visited Nov. 19, 2024). For example, Article 88 of the GDPR specifically permits member-states to provide "more specific

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.

---

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).

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 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

75. *See id.* arts. 44–50.

76. *See id.* art. 44.

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 (Feb. 24, 2023), 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).

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 upon the Privacy Shield, the DPF requires personal information being transferred

---

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.

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]

---

84. European Commission Press Release, Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows (July 9, 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, PRIVAZY PLAN, https://www.privacy-regulation.eu/en/recital-26-GDPR.htm (last visited Nov. 19, 2024).

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

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 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

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, PRIVAZYPLAN, https://www.privacy-regulation.eu/en/r47.htm (last visited Nov. 19, 2024).

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

90. *Id*.

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

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.

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

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.

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 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. 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]

---

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*.

The requirements to comply with these provisions and avoid civil or criminal liability similarly impact 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 that 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.

---

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 predate 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

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

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), implement necessary protective measures (due diligence, contractual protections, and monitoring), ascertain the above-mentioned explicit consent, and conduct 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]

---

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).

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

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 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]

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

Cross-border discovery might be further complicated because 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, 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 use 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.

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 Nov. 19, 2024).

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 the 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 fulfilling the legitimate interests of a

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

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 guarantees of protection (standard contractual clauses, 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 comprising two separate and independent systems for the taking of evidence abroad. Chapter I outlines the taking of evidence through

---

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).

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 used, 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 use of the other. They are self-contained in that the steps involved for each are unique to each and cannot 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 seeks 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 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 use 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

115. Id. at 8.

116. *Id.* at 10–16.

117. *Aérospatiale*, 482 U.S. at 547.

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]

---

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*, 2019 WL 6134958, at *4 (same).

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]

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

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*, 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.

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

---

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, 339 F.R.D. 487 (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) (quoting *Richmark*, 959 F.2d at 1475, "Where the evidence is directly relevant . . . this factor weighs against utilizing Hague procedures.") (quotations omitted).

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

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

---

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).

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 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]

---

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).

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.

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]

---

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.

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

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. Some courts conflate the proportionality and comity analyses, and still others 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 feed 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

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

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 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

---

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).

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

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 packages 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

144. *Id.* at 566.

145. 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*.

first establishing the foreign law conflict, and then weighing *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]

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

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).

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.

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

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.

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 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]

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).

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*,[160] 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.[161]

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 whether information is important to the litigation (which is the first *Aérospatiale* factor).[162] 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.[163]

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, 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

160. 486 F. Supp. 2d 1078, 1081 (N.D. Cal 2007).

161. *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).

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

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

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.'"[164]

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."[165]

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 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

164. 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).

165. 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).

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 . . . ."[166]

In *In re Xarelto (Rivaroxaban) Products 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.[167]

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

167. *In re* Xarelto (Rivaroxaban) Prods. 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.[168]

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 attach to the otherwise relevant discovery—only that the proportionality factors 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.[169] In that proportionality analysis, parties should articulate, and courts should

168. "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).

169. "So, the Court cannot endorse a simplistic holding that documents about foreign conduct are always relevant or never relevant because neither

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.[170]

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 a 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.

---

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).

170. "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.

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.[171] Relative access to relevant information and party resources, for example, is not as straightforward in a cross-border context as it 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 monetary and nonmonetary cost factors are appropriate "burdens" to consider.[172]

---

171. 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.

172. 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.").

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[173] and proportionality considerations, neither is it variable in concept. [174] It is 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.

---

173. 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.

174. "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).

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 it is listed here as an initial threshold consideration after relevance and privilege.[175] 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 that 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

175. 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*].

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 discovery."[176] 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 assist requesting parties 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 the 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

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

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 the 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.

c. Amount in Controversy

As a proportionality factor, the 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 heavily relied upon 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."[177] 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, 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.[178] Responding parties should have more information about the dis-

177. *Id*.

178. *Id*.

coverable information located outside the U.S., but it doesn't always mean 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 standard contractual clauses 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.

In terms of "relative access," the above challenges 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 responding 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 that meaningful Rule 26(f) conferences cannot occur without addressing them.

Parties that in good faith apply The Sedona Conference's recommended "actual ability to obtain"[179] standard to cross-border

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

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

(1) Privacy, Monetary, and Nonmonetary Cost 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 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.[180]

180. 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

For example, in *Johnson v. Nyack Hospital*, 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."[181]

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

---

in resolving the issues, and whether the burden . . . of the proposed discovery outweighs its likely benefit." *Primer on Social Media, Second Edition*, *supra* note 175, at 27–28.

181. Johnson v. Nyack Hospital, 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).

questions of proportionality often arise in the context of disputes about the expense of discovery, proportionality is not limited to such financial considerations.[182] 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.[183]

Some commentators have argued that privacy should not be considered an element of the proportionality analysis—especially as a nonmonetary 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).[184]

> 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

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

183. *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.").

184. "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 168, at 409.

> 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 nonmonetary cost factor specifically, include: privacy is a separate consideration from proportionality; proportionality should focus on economic or monetary costs;[185] Rule 26(c) is more flexible and lends itself to more consistent and transparent decision-making;[186] privacy could have been included in the 2015 amendments to Rule 26(b) but was not;[187] and consideration of privacy as an element of the proportionality analysis could actually dilute privacy protections.[188] As Hon. James C. Francis IV (ret.) points out, *Henson* and

185. 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 168, at 400.

186. Rosenthal & Gensler, *supra* note 184, at 78–79; *see generally* Francis, *supra* note 168.

187. "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 184, at 80.

188. "[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

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)."[189]

Robert Keeling and Ray Mangum, on the other hand, recognize that courts still tend 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.[190] They point out that the 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."[191]

This *Commentary* does not attempt to resolve whether privacy is or should be considered as its own factor in Rule 26(b) but simply recognizes 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

---

alongside privacy, does the value assigned to privacy interests in a particular case become apparent." Francis, *supra* note 168, at 426.

189. *Id.* at 417.

190. "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 181, at 426–27.

191. *Id.* at 424.

amounts or metrics but are very real. Addressing compliance with data protection obligations is both a legitimate monetary and nonmonetary cost burden, apart from the specific "privacy" rights of any given individual.

(2) Monetary 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 the 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.[192] The

192. *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 . . . .").

controller needs to inform the data subject/individual that his data will be processed,[193] 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," and "where 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.[194] 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 out-

193. *Id.*, art. 13(1)–(2).

194. Jeff Griffiths, *5 Questions About Cross-Border Discovery*, DELOITTE, https://www2.deloitte.com/us/en/pages/financial-advisory/articles/five-questions-cross-border-discovery.html (last visited Nov. 19, 2024).

side counsel/vendors, to engage in additional meetings to investigate potentially relevant data sources in other jurisdictions and potentially implement additional security measures (such as standard contractual clauses) 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.[195]

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.

(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

195. *International Litigation Principles*, *supra* note 2, at 16.

laws and regulations can severely restrict their legal ability to preserve personal data."[196]

In Europe, there are obligations toward the data subject/individual impacting preservation efforts.[197] The controller needs to inform the data subject/individual that his data will be processed,[198] 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," and "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 spend 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

196. *Commentary on Managing International Legal Holds*, *supra* note 10, at 166.

197. *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 . . . .").

198. *Id.*, art. 13(1)–(2).

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
- 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"[199]

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.

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

(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[200] 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 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

200. Early data assessments typically involve using data analytics and advanced electronic discovery 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.

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 jurisdictional requests for production sets that might subject documents to different privilege protections than those they were analyzed for during their original production.[201] 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 that 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 that outside counsel specializing in cross-border privilege law may have to be involved.[202]

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.[203] It is not just a relevancy

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

202. *Id*. at 507–32.

203. Article 29 Data Protection Working Party, Working Document 1/2009 on pre-trial discovery for cross border civil litigation, at 11 (Feb 11, 2009),

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 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 proficiency in other languages and higher per-hour billable rates.

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

---

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.

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.[204]

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

204. *International Litigation Principles*, *supra* note 2, at 20–21.

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.[205] 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."[206] Anonymization and pseudonymization are expensive.

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).[207] 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.

205. EDPB Guidelines 2/2018 on derogations of Article 49, *supra* note 93, at 12.

206. *Id*.

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

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.[208] 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 confidential, so a transfer outside those countries is not possible without the approval of the 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 also accessing production sets may increase costs. As noted above, additional costs

208. *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 . . . .").

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 in a given matter, cross-border discovery generally costs more in attorney and vendor fees. Discovery, disclosure, data protection and privacy 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, standard contractual clauses (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.[209] 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

209. *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 Nov. 19, 2024).

basic engagement increases. Completing Transfer Impact Assessments can further drive counsel and vendor engagement costs upward.[210]

(3) Nonmonetary Cost Factors

Parties and non-parties may also be impacted by nonmonetary factors both unique to and amplified by cross-border discovery, such as:

- 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.

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

- Adapting discovery workflows to include consultation with data protection officers and/or counsel.
- General cultural, language, and communication differences.
- Reputational damage and risk management concerns associated with noncompliance with data protection laws.
- Potential fines or criminal liability.
- Changing 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 nonmonetary 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 also 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.

Even though 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, nonmonetary factors as part of the Rule 26(b)(1) proportionality analysis to the extent that they present as actual burdens on the discovery process.[211] This is important whether an argument is made for protection of privacy as a right in the discovery process.

211. "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 20, 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 first 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.[212]

---

212. 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/3b290a7b-3885-4481-86c5-f8289f4ee759.pdf.

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

Although this *Commentary* recommends that parties facing transfer restrictions impacting necessary and proportional discovery explore transfer through the appointment of a Commis-

---

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 137–46.

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 la République 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.

sioner under Chapter II of the Hague Convention, it also recommends that this option only be engaged when the parties agree, 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 an 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 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.

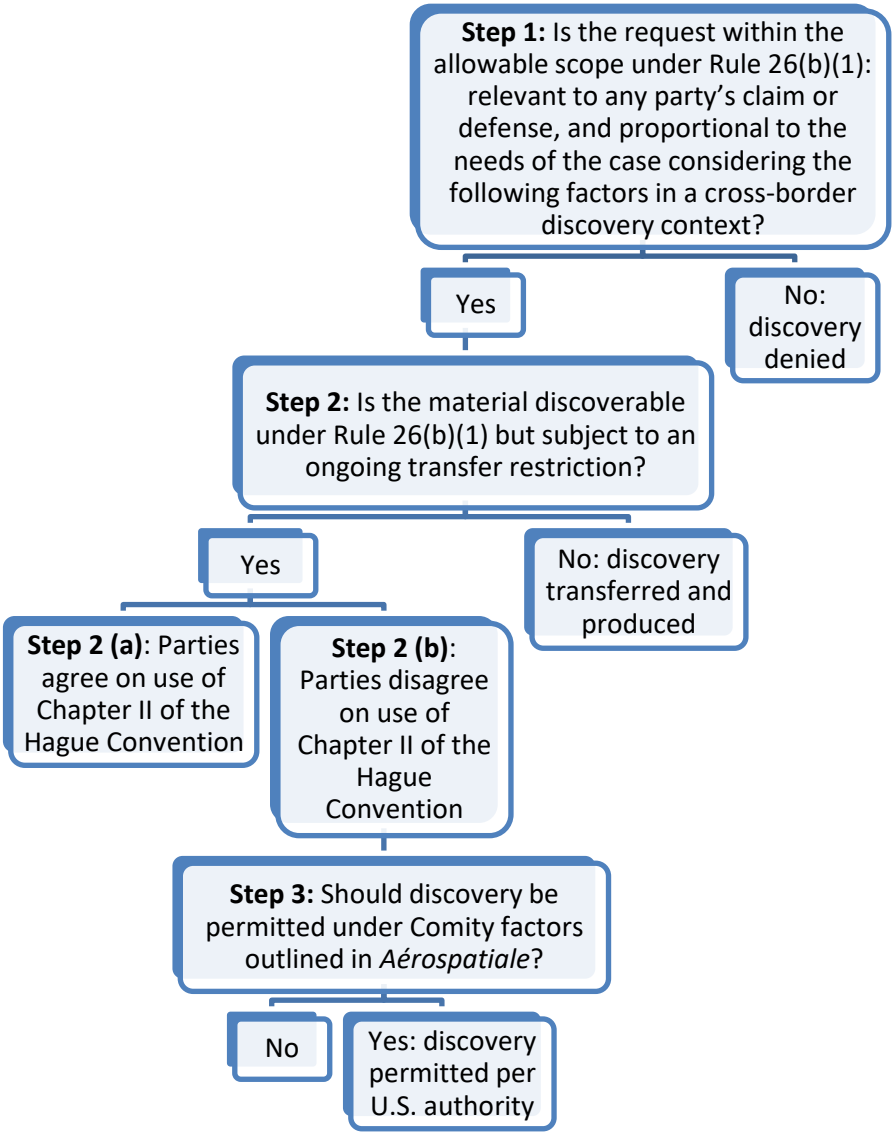
In contrast, the comity analysis outlined in *Aérospatiale* is specifically intended to address the interests of foreign sovereigns, which are generally not represented in the litigation. These principles are particularly important when the rights of foreign data subjects are at issue, as they are when 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 managing their dockets, but also for 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 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 bur-

densome, 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[213]

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 the close of the 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 allow sufficient time to implement data protection safeguards

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

---

213. *See International Litigation Principles*, *supra* note 2, at 39–58.

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, confer and negotiate with data protection authorities, conduct labor law assessments, and negotiate with employee Works Councils. Parties may also highlight heightened costs associated with international electronic discovery 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 at 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 Conven-

tion, 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 unnecessary.

Practice Point 6: Courts may minimize analytic and doctrinal problems relating to the 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 monetary and nonmonetary 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.

VIII. CONCLUSION

Balancing U.S. discovery rules with foreign data protection laws requires a nuanced understanding of proportionality and comity. In today's world of global cloud computing and continuous cross-border data movement, it is critically important for both attorneys and data protection experts to be not only aware of but well-versed in the varied laws and regulations impacting client approaches to relevant ESI in discovery workflows. Managing legal risks associated with discovery and data protection noncompliance requires practitioners to remain broadly knowledgeable about the multiple and often disparate demands of jurisdictional specific rules regarding ESI. Such knowledge, however, is both necessary and insufficient.

This *Commentary* emphasizes that the tendency of attorneys and courts to focus exclusively on the higher order—and often thornier and more time-intensive—legal challenges associated with questions of comity and choice of law is both self-defeating and out of step with Rule 26(b)(1) and ultimately Rule 1, particularly in today's environment. Parties and courts must first engage in a more rigorous scoping analysis. It is the common failure of attorneys to think through the practical aspects of cross-border discovery, data protection compliance, and proportional scoping that leads to unnecessary delays, motion practice, discovery disputes, and comity analysis.

Whether data protection and privacy should be a new factor in Rule 26(b)(1) is secondary to the reality of data protection burdens associated with cross-border discovery. While leveraging the Hague Convention and addressing true jurisdictional disputes through comity analysis is often necessary, those analyses should benefit from exhaustive and realistic proportionality and scoping considerations for the benefit of not just the responding party, but also the requesting party and the court's docket.

As shown in this *Commentary*, U.S. discovery rules, practices, and interpretations are not fixed and inelastic. They are tethered to the formats, volumes, and technological challenges of relevant information inherent in current times. Using a serial approach that faces these challenges directly and practically, instead of abstractly, will lead to more parties getting the specific discovery they need in less time and with less risk of noncompliance.

FRAMEWORK FOR ANALYSIS OF VENUE SELECTION FOR GLOBAL PATENT LITIGATION: STRATEGIC CONSIDERATIONS

A Project of The Sedona Conference Working Group on Patent Litigation Best Practices (WG10)

Author:

The Sedona Conference

Editor-in-Chief:

Matthew Powers

Managing Editors:

Jim W. Ko

Casey Mangan

Chapter Editors:

Ronald A. Antush

Tilman Müller-Stoy

Beatriz San Martin

Anthony Trenton

Contributing Editors:

Roeland Grijpink

Haifeng Huang

Amandine Métier

Roberto Rodrigues

Staff Editor:

David Lumia

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference's Working Group 10. They do not

necessarily represent the views of any of the individual participants or their employers, clients, or any organizations to which they may belong, nor do they necessarily represent official positions of The Sedona Conference.

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, click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> The Sedona Conference, *Framework for Analysis of Venue Selection for Global Patent Litigation: Strategic Considerations*, 25 SEDONA CONF. J. 779 (forthcoming 2024).

PREFACE

Welcome to the December 2024 Final, Post-Public Comment Version of The Sedona Conference's *Framework for Analysis of Venue Selection for Global Patent Litigation: Strategic Considerations*, a project of The Sedona Conference Working Group on Patent Litigation Best Practices (WG10). 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 complex litigation, intellectual property rights and artificial intelligence. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

WG10 was formed in late 2012 with a mission "to develop best practices and recommendations for patent litigation case management" and works closely with WG9 in its mission to "clarify and guide the evolution of patent damages and remedies." Both Working Groups' members represent all stakeholders in patent litigation.

The *Framework for Analysis of Venue Selection for Global Patent Litigation: Strategic Considerations* ("*Framework*") drafting team was launched in 2019, and the draft was a focus of dialogue at the WG9&10 Joint Annual Meeting in Philadelphia, Pennsylvania, in March 2019; the WG9&10 Joint Annual Meeting, Online, in November 2020; the WG9&10 Joint Annual Meeting, Online, in November 2021; the WG9&10 Joint Annual Meeting in Boston, Massachusetts, in June 2022; the 2023 Sedona Conference on Global Intellectual Property Litigation in London, UK, in January 2023; and the 2024 Sedona Conference on Global Intellectual Property Litigation in Munich, Germany, in March 2024.

This *Framework* represents the collective efforts of many individual contributors. On behalf of The Sedona Conference, I thank Chapter Editors Ronald A. Antush, Tilman Müller-Stoy,

Beatriz San Martin, and Anthony Trenton, who have led this drafting process and have reviewed the comments received through the Working Group Series review and comment process. I also thank Editor-in-Chief Matthew Powers, who serves as WG9&10 Chair Emeritus, for his oversight. I further thank everyone else involved for their time and attention during the drafting and editing process, including the Contributing Editors Roeland Grijpink, Haifeng Huang, Amandine Métier, and Roberto Rodrigues.

The statements in this *Framework* are solely those of the nonjudicial members of the Working Group; they do not represent any judicial endorsement of the recommended practices.

The *Framework* will be regularly updated to account for future significant developments impacting this topic. 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.

Kenneth J. Withers
Executive Director
The Sedona Conference
December 2024

TABLE OF CONTENTS

FOREWORD

Increasingly, the most significant patent disputes are global in scope, involving multinational corporations and international activities. Because the substantive and procedural laws of relevant countries are often quite different—for example, regarding the availability of rapid injunctive relief or significant damages—parties strategize how to exploit those differences to their advantage.

The overarching Principle for all of The Sedona Conference's current and forthcoming consensus, nonpartisan Commentary drafting team efforts in the global patent litigation space is as follows:

> **<u>Principle No. 1</u> – WG10 is developing Principles and Guidelines to permit litigants to identify the venues best suited for resolution of their global patent portfolio disputes and to litigate them in a fairer and more efficient manner for the benefit of all stakeholders in patent litigation, including both bench and bar.**

The overall purpose of The Sedona Conference**'s** global patent litigation efforts is to provide information and guidance to counsel, parties, and the courts on how to protect jurisdictional integrity and improve the transparency of international litigation practices.

The Sedona Conference Framework for Analysis of Venue Selection for Global Patent Litigation: Strategic Considerations presents the key procedural, substantive patent law and economic considerations driving venue selection of a patent holder seeking to enforce its global patent portfolios, as well as patent revocation actions and declaratory proceedings.

Matthew Powers
Editor-in-Chief
Chair Emeritus, Working Group 10 Steering Committee

Ronald Antush
Tilman Müller-Stoy
Beatriz San Martin
Anthony Trenton
Chapter Editors

I. INTRODUCTION

The Sedona Conference Framework for Analysis of Venue Selection for Global Patent Litigation: Strategic Considerations ("*Framework*") provides patent practitioners and patent litigants with insight about the factors that drive patent litigation toward some of the principal venues for such litigation, in the hope that such information will permit litigants to identify the venues best suited for resolution of their dispute. With this *Framework*, WG10 also attempts to provide patent policymakers with insight as to how this variety of adjudicatory regimes influences the behavior of litigants in innovation-driven industries when they face disputes that are not resolvable without litigation.

To this end, this *Framework* summarizes and compares the procedures and relief available in seven principal international patent venues and considers the strategic and tactical factors informing the choice of various venues. These issues will be addressed from the perspective of the different types of plaintiffs and defendants likely to engage in international patent litigation, including parties engaged in competitor litigation, parties engaged in litigation brought by practicing entities seeking to maximize the value of their patent assets, and parties engaged in litigation brought by nonpracticing entities (NPEs) seeking to maximize their return on their patent investments. Current trends in venue selection will also be addressed.

The principal venues that will be considered are the United States, Brazil, United Kingdom, Germany, The Netherlands, France, and China.

Section II of this *Framework* presents the seven key drivers for global venue selection. The *Framework* identifies the procedural and substantive patent law and the economic considerations driving the venue selection of patent holders seeking to enforce their global patent portfolios.

Section III presents the factors that a prospective patent infringement defendant may take into consideration—some overlapping with those of the patent plaintiff and some unique to the patent defendant.

Section IV presents a survey of the seven identified principal patent litigation venues with respect to practices, procedures, and substantive and remedial rules that are relevant to venue selection and with respect to the current trends and advantages and disadvantages of litigation in each venue.

II. KEY DRIVERS FOR GLOBAL PATENT VENUE SELECTION

With the globalization of markets and supply chains, patent disputes are increasingly likely to play out in multiple jurisdictions around the world. While patents are filed in a wide range of jurisdictions, patent owners and prospective defendants often pursue lawsuits in parallel only in a few strategically selected venues.

This *Framework* examines seven factors that patent owners (and potential defendants, see Section III below) may consider when they evaluate and select venues for the litigation of global patent disputes:

1. The market
2. Quality of adjudication
3. Time to trial and final relief
4. Likelihood of prevailing on the merits
5. Availability of effective relief
6. Cost of litigation
7. Recovery of fees

A given factor may be more or less significant depending on the type of litigants and the type of controversy.

A. The Market

The relevance of the market—whether it's the place where accused products are manufactured or sold or where the defendant is located—is one of the first factors in evaluating and selecting venues for patent infringement cases. The United States, Brazil, Europe, and Asia (particularly China) have been important manufacturing regions and sales markets for multinational firms and are considered the top venues for patent disputes.

The accused infringement needs to be established in the relevant market; otherwise, the patent case may be dismissed

for lack of jurisdiction. More important, the degree of presence of the defendant or its affiliates or partners in the relevant market will also affect the level of pressure that can be generated against the defendant. An early settlement favorable to the plaintiff is more likely if a locally granted injunction can be enforced against the local defendant and result in the shutdown of factories that make and supply the infringing products.

The size of the market also matters. A larger market leads to more significant damages levels and leverage for the plaintiff in patent cases relating to the sale of products. Relatedly, another important consideration for patent litigation is the extent of imports. An exclusion order from the U.S. International Trade Commission (USITC) can effectively prevent the infringing products from entering the U.S. market. The extent of exports is also a significant factor. In particular, the Chinese courts will enjoin the export of infringing products made in China, which in many cases can result in a global impact for industries or firms that have their manufacturing or assembly base in China.

B. Quality of Adjudication

Quality of adjudication is an important factor in evaluating and selecting venues for patent litigation.

The track record and predictability of a venue are important considerations. Bringing proceedings in courts in venues with a substantial track record for patent litigation sends a stronger signal than in courts not known for their patent expertise. Moreover, filing patent cases before a court with extensive experience can minimize the uncertainty for both sides. This is particularly true for cases involving certain issues or subject matter, such as standard-essential patents or biotechnology. On the other hand, in some cases, a party may decide to take a blitz approach and seek to obtain an injunction in multiple places—

anywhere with a sizeable market—irrespective of certainty, in order to maximize its chances.

Overall reputation and general attitude toward patents in the venue are also important. In practice, certain venues have been generally preferred by litigants. For example, in the U.S., particularly in the technology space, the District of Delaware, the Eastern District of Texas, and more recently the Western District of Texas have been favored among licensing companies or NPEs, while the Northern District of California is preferred by defendants; whereas the Districts of New Jersey and Delaware are popular and experienced in handling pharmaceutical cases. In Europe, Germany (Düsseldorf and Mannheim), the UK, France, and the Netherlands are preferred. In Asia, China's Intellectual Property (IP) system has gained popularity among patent owners since the rollout of specialized IP courts in Beijing, Shanghai, and Guangzhou in 2014 (and most recently the establishment of a single, national appellate court for patent cases in 2019). Japan and Korea are also common venues.

Finally, the presence in the venue of experienced outside counsel and technical advisors to assist with the adjudication is another important factor. It is critical to find and manage outside counsel on the ground that can effectively present the cases to the local judiciary and also seamlessly coordinate with firms and advisors in different venues. It is also important to identify and confirm if technical advisors (in some places put forward as expert witnesses, technical investigators, or appraisal institutes) with the necessary expertise on the patented technology are available in the chosen venues, particularly in countries where there may be a perceived heightened preference for local experts.

C. Time to Trial and Final Relief

The time to "relief"—whether that relief is a preliminary injunction, a final decision and damages award from a first-instance court or appellate decision, a permanent injunction issued from a first-instance court, or a final appellate decision—is a critical factor in evaluating and selecting venues for a patent infringement case. Likewise, for a prospective defendant, the time to invalidation of the patent or grant of a declaration of noninfringement is important. Which one (or more) of these relief milestones is most important in a particular instance will depend on the nature of the litigant and its legal and business objectives. But to be attractive, a venue must be one where the litigant can reach the relief milestones that are most important to it in a reasonable (and reasonably predictable) time frame. Below are some matters to consider in evaluating a venue's attractiveness from a timing perspective.

The first potential relief milestone in a patent infringement case is a preliminary injunction.[1] With respect to timing, if a venue has a procedure for a patent owner to obtain a preliminary injunction and such injunctions are available as a practical matter, a preliminary injunction can be a very powerful form of relief. But in most jurisdictions, a patent owner will have to present a very strong case on the merits or show irreparable harm to obtain a preliminary injunction. In some venues, these and other requirements rule out preliminary injunctions in most cases. But in jurisdictions where the time from the filing of the complaint to a final decision in the first-instance court is typically many years, seeking and obtaining an early preliminary injunction may be the only effective relief available.

1. Preliminary injunctions and similar preliminary relief, such as seizures, are discussed in more detail *infra* Section II.E.3.

The time to a first-instance final decision is the milestone by which most patent owners will evaluate the efficacy of a venue, because it is the milestone that can provide the patent owner with a "win" and potentially a significant damages award and permanent injunction. The time to this milestone varies dramatically from venue to venue. For example, in the United States, the median time to trial in patent cases is 30 months, but it can be as much as three to four years in some jurisdictions, and as little as nine to 12 months in others. If a patent owner can satisfy the requirements for filing a case in the USITC,[2] the case can go from start to finish in less than 18 months. Many other major patent venues (e.g., Germany, China, and the United Kingdom) are much faster than the U.S.—particularly civil law jurisdictions where there are specialized patent courts and little or no discovery. But, as discussed elsewhere in this *Framework*, the lack of discovery in civil law jurisdictions and the low level of damages awards (as compared to the U.S.) may make some of these jurisdictions less attractive, or at least require a patent owner to consider a multijurisdictional approach.

An important and sometimes overlooked factor in evaluating the time to a final first-instance decision is whether the case, as a matter of law, can be stayed pending completion of separate patent office or patent court invalidity or nullity proceedings filed by the defendant; and, if so, the likelihood that the case will actually be stayed. Laws and practices regarding stays vary significantly across venues. For example, in the United States, since the advent of the inter partes review (IPR)

2. For an overview of USITC litigation, *see* The Sedona Conference, *Commentary on Patent Litigation Best Practices: International Trade Commission Section 337 Investigations Chapter*, (May 2019), https://thesedonaconference.org/publication/Commentary_on_Patent_Litigation_Best_Practices_ITC_Section_337_Investigations.

process in 2012,[3] it has become common for patent defendants to file IPR petitions as quickly as possible after being sued, and then (if the Patent Office agrees to hear the IPR; which happens about 60 percent of the time) to request that the court stay the infringement case pending the completion of the IPR process, which typically takes 18 months. The success rate of such stay motions varies widely by jurisdiction, but overall, about half are successful. The practical effect of an IPR-based stay, particularly if granted when the case is at an early stage, is that if the IPR is unsuccessful, the litigation does not start moving ahead until two (or more) years after it is filed. Having a case stayed for two-plus years is normally very disadvantageous for a patent owner. However, invalidation of a patent in an IPR procedure is not a foregone conclusion, and a patent that survives IPR review will be materially less vulnerable to invalidation in a district court proceeding.

In contrast to the U.S., in Germany's bifurcated system, the infringement court generally will not stay an infringement case pending the outcome of a nullity proceeding before the German Patent Court (or European Patent Office opposition proceedings). However, in rare cases, if there is a very strong piece of prior art that is likely novelty-destroying and that has not been cited in prosecution, the infringement court will stay the proceedings and not grant the otherwise presumptive injunction. There has been a slight trend in Germany toward granting more stays, particularly where the patent owner is a

3. For an overview of the USPTO Patent and Trademark post-grant proceedings, including the IPR process, *see* The Sedona Conference, *Commentary on Patent Litigation Best Practices: Parallel USPTO Proceedings Chapter ("Stage One")* (Oct. 2016) *and* The Sedona Conference, *Commentary on Patent Litigation Best Practices: Parallel USPTO Proceedings Chapter ("Stage Two")*, Public Comment Version (July 2017), [hereinafter *Sedona Parallel USPTO Proceedings*], https://thesedonaconference.org/publication/Parallel_USPTO_Proceedings, and Section IV.A.1.b.

nonpracticing entity. In China, court proceedings typically won't be stayed pending the completion of a nullity proceeding before the Patent Review Board unless the asserted patents are utility model patents or design patents that were granted in China without substantive examination. In any case, the legal and practical availability of a stay is something that every patent owner should take into account in selecting venues.

Even if it is possible to obtain a prompt first-instance or final court decision in a particular jurisdiction, a patent owner must also consider what the immediate legal and practical value of a favorable trial or first-instance infringement judgment (and, if applicable, a permanent injunction) will be. For instance, in some jurisdictions (e.g., China), damages awards and permanent injunctions are generally stayed pending the outcome of an appeal. In other venues (e.g., Germany), where injunctions are automatic, if the patent owner wants the injunction to take effect immediately and remain in effect during the pendency of any appeal by the defendant, it must post a bond. The required bond amount can be substantial, sometimes prohibitively so.

Furthermore, in many jurisdictions, the assessment of damages is bifurcated from the assessment of liability. Accordingly, damages are not awarded until a considerable period of time after the court has established liability. If an injunction is granted immediately, the patent owner may be able to leverage that in order to secure a resolution involving payment of damages. If not, the patent owner will need to wait until the outcome of the damages phase of the proceedings before any damages are awarded.

Moreover, in most jurisdictions, an adjudicated infringer's obligation to pay the damages awarded by the first-instance court will be stayed pending appeal if the defendant posts a bond to secure the damages amount. Thus, for a patent owner

whose primary goal in a litigation is to collect money, the patent owner will not be able to get that money unless and until the infringement judgment and damages award are affirmed on appeal.

Finally, in evaluating the time to relief (particularly in venues where permanent injunctions are difficult to obtain or generally stayed pending appeal), a patent owner will consider the length of the appeal process in the venue. Even in the fastest jurisdictions, the time from the filing of an appeal to an appellate decision is 12 to 18 months; in many jurisdictions, the period is much longer. Patent owners may decide that a process that takes four or more years from filing of the complaint to the final appellate decision does not provide practical relief. Accordingly, a prudent patent owner will evaluate carefully whether a venue can provide it with timely relief based on its legal and business objectives.

D. Likelihood of Prevailing on the Merits

Even if a venue is favorable for litigants from a timing perspective, it may nevertheless not be an attractive venue if it is not one where a litigant has a reasonable chance of prevailing on the merits of its case. Obviously, a significant factor in whether a litigant can win is the intrinsic quality of the patent (novelty, inventive step, quality of specification, quality of claims, etc.) that is at issue. Without these attributes, a patent owner should and usually does lose, regardless of the venue. But assuming that the litigant has a strong case on the merits, there are a number of other factors that are considered in evaluating venues. First among these is whether the venue provides a fair and impartial forum for adjudication of patent disputes. Questions to consider here include whether the judiciary is independent and decisions are made on the merits, rather than on "extrajudicial" factors such as political influence or corruption. A litigant that is not based in a country in which

it is considering litigation must evaluate whether its case will be decided fairly and on the merits, particularly where the opposing party is a domestic company. For example, will the court be willing to enter an injunction against a large domestic company? Conversely, will the court be willing to find the patent was not infringed if the patent holder is local and the defendant is not?

Litigants should consider the quality of the patent judiciary in the venue as discussed in Section II.B above. Questions here include: Are there specialized intellectual property courts, such as in China, Germany, the United Kingdom (UK), France, and the Netherlands? And, if (as in the United States) there is not a specialized patent judiciary, are there other factors that enable the litigant to have confidence that the court will be able to understand and competently decide infringement (and, if applicable, validity)?

Third, for jurisdictions in which there is little or no discovery, a patent owner must ask whether it can prove infringement with the information otherwise available to it (such as with evidence preservation orders). For process-patent cases in particular, this can be quite difficult.

Finally, a patent owner will consider whether a venue provides protection for the technology at issue. Countries have different levels of protection for various technologies, such as software and diagnostic technologies, and in some cases the law is evolving. Of course, if the country does not allow patents on a certain technology, then the patent owner presumably will not have patents on that technology in that country. But even if the country allows for patents on a technology, the patent owner will evaluate whether the courts in that country are likely to *enforce* the patents covering that technology and issue an injunction if infringement is found. For example, most countries allow patents to be obtained on pharmaceuticals, but some

(particularly newly developing countries) have shown a reluctance to enforce and, in particular, grant injunctions against infringement of pharmaceutical patents. European countries have a reticence concerning technology involving embryos. The United States has limited protection for medical diagnostics. In China, methods for diagnosis or treatment of diseases are not patentable, but software is patentable.

In sum, in addition to the patent merits, there are a host of other factors a litigant will consider in evaluating venues for patent litigation.

E. Availability of Effective Relief

The availability of injunctive relief is often a key factor for a plaintiff choosing a specific patent litigation venue. An injunction may be used to put a defendant out of the infringing business, increase the patent owner's market share, or serve as a strong settlement lever in the plaintiff's favor. In extreme cases, an injunction can even lead to elimination of a competitor in the relevant market sector. In most, if not all, venues outside of the United States, an injunction will generally follow a finding of infringement. In the United States, the availability of injunctive or injunction-like relief will often depend on the competitive posture of the litigants (competitors, for example, are relatively likely to secure injunctive relief, particularly in competitor v. competitor disputes) and the jurisdiction that is hearing the dispute (the USITC, for example, almost universally grants injunction-like importation bans on infringing products).

1. Availability of Substantial Damages

The availability of damages, compared to an injunction threat, generally plays a secondary role in the decision where to start patent litigation proceedings. Particularly in venues where damages are limited to compensatory damages, the availability

of such damages is usually not a key driver in the choice of venue but rather a positive side benefit of a successful patent litigation. In the United States, however, the level of damages awards, typically higher than elsewhere, is a key driver for bringing proceedings there. Damages can be very significant in high-stakes cases, particularly when enhanced damages are available (such as punitive damages and treble damages for willful infringement).

Data for damages awards in patent litigation around the world is difficult to obtain, as parties often settle on damages if liability is established.[4]

2. Availability of Preliminary Relief (e.g., Preliminary Injunctions and Seizures)

In jurisdictions where injunctions can be obtained, the availability of preliminary relief can, in particular cases, be a key driver for a plaintiff choosing a specific venue. However, plaintiffs usually consider this more a useful tool and a positive side benefit of an already chosen venue. A preliminary injunction primarily makes it possible to obtain and enforce the injunction quickly. Also, it sometimes allows the plaintiff to obtain information about the origin of the infringing product and its distribution channels. A plaintiff will consider a preliminary injunction to be a particularly useful strategy for stopping ongoing infringement immediately when there is no compensation obtainable by way of damages. This is typically

4. For a survey identifying judgments granting damages for patent infringement in the six most active European countries in patent litigation (Germany, Spain, France, Italy, the Netherlands and the United Kingdom) between 2000 and 2019, *see* Pierre Véron, *What Price Crime? A European hit parade of patent infringement damages*, GRUR 2/2021 (Feb. 2021), pp. 392–96, *available at* https://www.veron.com/wp-content/uploads/2021-02_GRUR_Pierre_Veron_Damages_patent_infringement_Festschrift_MeierBeck.pdf.

the case in the run-up to or during important trade fairs, or in the case of a competitor launching a new infringing product. Vis-á-vis trade shows and pharma cases, plaintiffs find that preliminary injunctions are particularly effective at preventing a competitor from market entry, e.g., launch of a specific drug or other pharmaceutical product.

Similar considerations apply for preliminary seizures. In addition to court proceedings for patent infringement, in some jurisdictions (e.g., the European Union[5] and China), it is also possible to prevent the import and export of infringing goods at the external borders by means of so-called customs seizure proceedings, which request the customs authorities to seize and eventually destroy infringing goods. From a practical perspective, the customs seizure proceedings that are available may be an interesting add-on to put pressure on a patent infringer in parallel to litigation. But customs seizure proceedings are usually not considered to be very effective as a stand-alone measure. A notable exception is USITC proceedings, which typically result in import bans and customs seizures that are a highly effective, nonpreliminary option.

F. Cost of Litigation

The cost of litigation varies widely among venues around the world. The common perception is that costs are significantly higher in common law jurisdictions than civil law jurisdictions. Some of the perceived difference may be exaggerated; however, there is no doubt that, for example, U.S. proceedings with extensive documentary discovery and oral depositions are more costly than litigation in France, Germany, and China, which have limited or no discovery.

---

5. One example is the *saisie contrefaçon* search and seizure mechanism available in France's legal system. For discussion, *see infra* Section IV.B.3.a.ii.

However, while the cost of litigation is a significant factor as to where (or even whether) small- or medium-sized cases should be initiated or defended, it is not a significant factor for venue determination in most multijurisdictional disputes. Such disputes, which tend to be global or at least highly international in scope, are of such a scale that the cost of the litigation itself will not determine the venue over the other considerations discussed here.

This is readily tested by the following example: most multijurisdictional litigation is brought in the United States in addition to other jurisdictions. The United States is a significant venue because of the size and quality of its market (leading to sizeable damages awards), as well as the quality of adjudication. However, it is without doubt the jurisdiction with the highest costs. If cost was a determining factor in venue selection, the U.S. would not be such a popular venue.

G. Recovery of Fees

Recovery of fees, i.e., recovery by the prevailing party of its attorney and patent attorney fees, court fees, and litigation expenses, is usually not a key driver for selecting a patent litigation venue in multijurisdictional litigation for the same reasons that the cost of litigation is not. However, for smaller or midsized companies, the risk that the other side could recover fees in larger scale cases might be prohibitive.

III. OPPORTUNITIES FOR DEFENDANT-INITIATED LITIGATION

Much litigation is initiated by prospective defendants in anticipation of litigation being commenced by the patent holder. It may be initiated by potential declared standard-essential patent defendants, or generic pharmaceutical companies, or any other potential defendant to patent litigation.

Traditionally, the approach taken by potential defendants has been to lie low and not take the initiative in commencing proceedings. After all, the patent holder may be hesitant to initiate litigation. That is particularly so if there are many potential defendants. Historically, the general view was that the potential benefits to a defendant of initiating litigation were outweighed by the disadvantages.

This approach likely still prevails in most cases; nonetheless, a prospective defendant may consider that there are strategic or tactical advantages in initiating litigation in some cases. The reasons for a defendant initiating patent litigation include:

- selecting the jurisdiction in which the proceedings are brought;
- delaying/blocking proceedings;
- obtaining an early positive result and improving the defendant's negotiating position;
- obtaining an early positive result and influencing the courts of other jurisdictions;
- bringing a counterattack to increase the pressure on the patent holder and avoid or settle the dispute; and
- "clearing the way" in advance of launch in jurisdictions where failure to do so is likely to lead to a preliminary injunction being granted upon launch.

Each of the factors discussed in Section II relevant to venue selection by patent holders will also apply to potential defendant-initiated litigation. Clearly, the size and nature of the market will be just as relevant to such litigation; generally, there is little point in a defendant initiating litigation where the market is of no significance.[6] The quality of adjudication is as important to the defendant as to the patent holder. The time to trial is also a crucial factor. In some cases, it may suit a defendant for the time to trial to be as quick as possible (for example, where the defendant hopes the result will influence the courts of other jurisdictions). The likelihood of prevailing on the merits is necessarily crucial, although its effect on venue selection may depend on the defendant's perception of the importance to the outcome of being "local." A further key factor is the availability of the various tools and procedures that may be deployed by a potential defendant. Jurisdictions around the world differ considerably as to what a potential defendant may initiate, and the circumstances in which they may do so.

The various forms of action that may be brought by a defendant are addressed below, according to the strategic or tactical reason for doing so. Additionally, European Patent Office oppositions are detailed briefly.

A. Selecting the Jurisdiction

Just as a patent holder will wish to select a venue based on the factors discussed above, so may a potential defendant. One way a potential defendant may try to do this is by seeking declaratory relief, such as a declaration of noninfringement. Within the European Union (EU), under the *lis pendens* rules in the Brussels Regulation, the court of the member-state in which

6. *But see infra* Section III.B, discussing the dilatory tactic for potential infringers called the "torpedo."

the defendant initiates its proceeding may then seize jurisdiction, thereby blocking any other EU jurisdiction from determining the matter. Accordingly, a defendant confident of its noninfringement position may also be able to seek a pan-European declaration of noninfringement. Other related forms of declaratory relief may also be available in certain jurisdictions, such as declarations of "nonessentiality" (in relation to declared standard-essential patents in the technology field). Whether such alternative declaratory relief is available will depend on a jurisdiction's approach to (a) the form of declaratory relief sought; and (b) who is entitled to claim it.

In the context of patent license disputes, once a declaratory judgment as to the effect of a license agreement has been obtained, it may be possible through estoppel doctrines to prevent the courts of other jurisdictions from considering the matter.

Another well-established approach to controlling jurisdiction has been for parties to obtain "anti-suit injunctions"—injunctions preventing a party from pursuing litigation in a foreign jurisdiction. These are relatively rare in the patent litigation sphere, which has traditionally taken a territorial approach. However, there have been some examples recently in the FRAND[7]-related standard-essential patent field. For example, anti-suit injunctions were granted in U.S. courts relating to foreign infringement claims in *Microsoft Corp. v. Motorola Inc.*[8] and in *TCL Communication Technology Holdings Ltd v. Telefonaktiebolaget LM Ericsson*.[9] Recently, the Munich district court issued an "anti-anti-suit injunction" preventing

7. Fair, Reasonable And Non-Discriminatory: a licensing commitment typically taken on by a patent owner when declaring its patent(s) as essential to practice a technical standard.

8. 871 F. Supp. 2d 1089 (W.D. Wash. 2012).

9. Order re Motions, No. CV 14-0341 JVS (ANx) (N.D. Tex. Aug. 9, 2016).

Continental from pursuing an anti-suit injunction in the U.S. that would in turn have sought to prevent Nokia from pursuing proceedings in Germany.[10]

B. Delaying Proceedings

Ordinarily, initiating litigation will not delay the dispute; quite the contrary, it will precipitate it. But one tactic—the "torpedo"—is an example of a proceeding instituted for the purpose of delay. While a torpedo could theoretically still be launched today, it has not been in common use for some time.

The "torpedo" is an action brought in an EU member-state to obtain a pan-European declaration of noninfringement, again relying on the effect of the *lis pendens* rules in the Brussels Regulation to seize jurisdiction Europe-wide. Under these rules, once an EU member state-court has been seized of a matter, it is not possible for another EU member state to take jurisdiction until the first court has decided it does not have jurisdiction.

Accordingly, a practice developed whereby proceedings seeking a pan-European declaration of noninfringement were brought in courts that had notoriously slow procedures (such as those in Italy or Belgium) and often took years to determine whether they properly had jurisdiction, let alone to rule on the merits. In the meantime, because the infringement issue was being considered by the first court, other courts were arguably blocked from considering it. "Torpedoes" were initiated without apparent regard for whether there were legitimate grounds for jurisdiction in the first court; the purpose was not to have that court ultimately determine the parties' substantive rights, but rather to delay other EU courts from doing so. In fact, the practical effect of the torpedo may not have been all that

10. Continental v. Nokia, Case No. 6 U 5042/19 (Munich Higher Regional Court 2019).

significant. Other member-states' courts found ways of progressing infringement actions despite the launch of any torpedo.

C. Obtaining a Positive Result to Improve Negotiating Position

In cases where a defendant has considerable confidence in its position, it may choose to bring proceedings itself in a favorable jurisdiction to obtain a credible early judgment to its benefit, with a view to settling the dispute worldwide on beneficial terms. To an extent, all litigation that is brought in a global scenario relies on developing a strong position to lead to settlement. After all, it is hardly possible to bring proceedings in every jurisdiction around the world. Sooner or later, the parties will resolve the dispute based on the results in key jurisdictions.

The various factors discussed above in relation to patent-holder-initiated litigation will apply in the selection. Because proceedings are likely to be brought by the defendant in a single jurisdiction (rather than several), the choice will be heavily weighted toward the jurisdiction perceived to give the best chance of obtaining a favorable judgment that may set an example.

Another key factor will be the availability in various jurisdictions of the relief sought by the defendant. The types of relief that a defendant may seek are mainly declarations of noninfringement (if the defendant is confident in the noninfringement case) and nullity/revocation actions (if the defendant is confident in the invalidity case). In some jurisdictions, both can be brought together. The requirements for bringing a declaratory action for noninfringement or a nullity action differ across jurisdictions. For example, in the UK, no locus is required to bring a nullity action, while in the U.S., locus is required.

In addition, some jurisdictions such as the UK are particularly flexible with respect to the types of declaratory relief that can be ordered. In the UK, there are no formal limits on what can be ordered, although a declaration does need to relate to contested legal rights and must have a practical purpose. For example, the UK will consider granting declarations of "nonessentiality" (i.e., that a patent is not essential to a standard) and so-called "*Arrow* declarations" (declarations that a particular product is obvious over the prior art as of a certain date, so that any patent granted in the future that covers that product necessarily lacks inventive step).[11] Accordingly, the availability of special forms of declaration may also be a determining factor in venue selection.

D. Obtaining a Positive Result to Influence Other Jurisdictions

The factors discussed above also apply to the goal of obtaining a result that might influence other jurisdictions. Just as the parties' global settlement of worldwide disputes may be based on a limited set of litigation results, so do parties expect that some jurisdictions will be guided by outcomes in other jurisdictions. Certain jurisdictions are more influential than others, particularly those with respected patent courts, such as the U.S., Germany, the UK, and the Netherlands. The key European jurisdictions are particularly influential on each other. Accordingly, the perceived quality of adjudication is a particularly significant factor in this regard.

One significant scenario in which proceedings are brought in one jurisdiction in the hope of influencing those in another is where invalidity proceedings are brought in one European jurisdiction (such as the UK or the Netherlands) to affect the

11. *Arrow* declarations are named after the case that first confirmed the court's jurisdiction to grant such relief. *See infra* Section IV.B.2.b (United Kingdom–Opportunity for Defendant-Initiated Litigation).

outcome in Germany. In Germany, patent proceedings are bifurcated. Infringement proceedings are brought in separate courts from the validity court (the German Federal Patent Court). Typically, infringement proceedings will be heard significantly before the validity proceedings (for example, a year before). If infringement is found, the district court will generally issue an injunction, even though no determination of validity has yet been made by the Federal Patent Court. The injunction may be stayed, however, if it can be shown that there is a high likelihood the patent is invalid, as discussed above. That usually means a defendant demonstrates there is a new piece of prior art (not previously cited in prosecution) that is likely to be found novelty-destroying. But another way defendants have persuaded the district court to stay the injunction is by demonstrating that a counterpart European patent has been found invalid by the courts of another European jurisdiction. German courts are required to consider such decisions from other European national courts.

Accordingly, a practice has developed whereby potential defendants in Germany bring invalidity proceedings in other influential European jurisdictions (typically the UK or the Netherlands), with a view to obtaining a rapid determination of invalidity that can be cited to the German district court in the event that infringement is established there. The invalidity proceedings in the other European jurisdiction must progress very rapidly to achieve this—i.e., a judgment needs to be issued in less than a year.

E. Bringing a Counterattack to Increase the Pressure on the Patent Holder

Another common strategy is for a potential defendant to assert its own patents (or other rights) against the prospective plaintiff. These patents may be relevant to the patented technology of concern, or they may be entirely unrelated. The

factors discussed above, in relation to patent-holder-initiated litigation, will apply equally when selecting the venue. Defendants can sometimes leverage positive outcomes in such counterattacks to help resolve the wider dispute on more favorable terms.

F. "Clearing the Way"

"Clearing the way" has a limited application to generic pharmaceutical litigation in the UK. In *SmithKline Beecham Plc. v. Apotex Europe Ltd.*, the English Patents Court held that if a generic pharmaceutical company (that will typically know its intended launch of a product several years ahead) fails to "clear the way" by either obtaining a declaration of noninfringement or revocation of a relevant patent in advance of launch, it will likely be subject to a preliminary injunction upon launch.[12]

In the UK, it is not straightforward to obtain preliminary injunctions in patent litigation. However, this is one exception. Accordingly, it is quite normal for generic pharmaceutical companies to bring actions for declarations of noninfringement or revocation actions a year or two before launch.

Somewhat analogously, the Hatch-Waxman statutory scheme in the U.S. provides a technique for generics manufacturers to secure a determination of whether their version of a small-molecule pharmaceutical will infringe the patents protecting the branded version of a drug before actually launching the generic product. More recently, the U.S. implemented a somewhat similar scheme relating to large-molecule drugs or "biologics."[13]

---

12. [2002] EWHC 2556 (Pat) (England and Wales High Court–Patents), *available at* https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Patents/2002/2556.html&query=(EWHC)+AND+(2556).

13. For an overview of biopharma litigation in the U.S., *see* The Sedona Conference, *Commentary on Patent Litigation Best Practices: Unique Aspects of*

G. Patent Office Oppositions

A further approach that prospective European defendants have taken is to bring a European Patent Office (EPO) opposition challenging the validity of a patent that is being, or may be, asserted against them. Oppositions may be brought within nine months of the date of grant. After that period, parties may intervene in opposition proceedings if the patent is being asserted against them, provided that an opposition is still pending when intervention is requested.

If successful, an EPO opposition has the effect of invalidating all national designations of the European patent. Oppositions are, however, relatively slow (in comparison with some national nullity proceedings) and can take several years, including the appeal to the Technical Board of Appeal. Note that it is not possible to bring nullity proceedings in the German Federal Patent Court if an EPO opposition is pending (contrary to some other European countries like the Netherlands or France), so this can be a factor for a defendant formulating its strategy when faced with an injunction in Germany.

The analogous U.S. procedure is to seek inter partes review in the Patent Trial and Appeal Board of the U.S. Patent and Trademark Office. This remedy was created as part of the 2012 revisions to the U.S. patent statute, known as the America Invents Act (AIA). An IPR procedure enables a litigant in a district court action to seek review of the validity of the patents in suit. Under appropriate circumstances, the district court may stay the action before it while the IPR process plays itself out. The effect of an IPR on pending infringement litigation can vary considerably. The IPR proceeding may end the litigation by

---

Biopharma Litigation Chapter, Public Comment Version (Oct. 2021), https://thesedonaconference.org/publication/Patent_Litigation_Best_Practices_Biopharma_Litigation.

invalidating the patent, narrow the litigation by invalidating certain claims or precluding reliance on certain prior art or certain validity defenses, delay the litigation while validity is reviewed, enhance the strength of the patent-in-suit, or leave the district court litigation wholly unaffected.[14]

14. For an overview of and Principles and Best Practice recommendations for practicing before the USPTO Patent Trial and Appeal Board in post-grant proceedings, *see Sedona Parallel USPTO Proceedings*, *supra* note 3.

IV. SURVEY OF KEY JURISDICTIONS

This *Framework* does not strive to offer a comprehensive discussion of the substantive and procedural rules applicable in each venue. Instead, it focuses on the aspects of each venue that affect its suitability for a particular controversy, applying the same factors presented in Sections II (Key Drivers for Global Patent Venue Selection) and III (Opportunity for Defendant-Initiated Litigation).[15]

A. The Americas

1. The United States

Because U.S. patent law is subject to exclusive jurisdiction in the federal courts, patent owners can bring an infringement suit in any of the 94 U.S. federal district courts of first instance over the manufacture or sale of patented items anywhere in the country, provided that personal jurisdiction and venue requirements are met. A high concentration of patent lawsuits, however, are brought in only a few of these district courts. In addition, a patent owner can bring a case asserting unfair acts of competition before the USITC, which has the authority to issue broad exclusion orders to stop the import of infringing products into the U.S.

In addition to being able to challenge the validity of any patents asserted against them before the presiding court, patent defendants (or potential patent defendants) can also challenge the validity of the patents in the U.S. Patent and Trademark

15. The existence and level of activity of a country's competition law or antitrust authority may well impact a global patent litigation and venue selection strategy, in particular in the enforcement of standard-essential patents. Such an analysis is outside the scope of this *Framework*.

Office's Patent Trial and Appeal Board using one of the post-grant proceedings established in the AIA.[16]

a. Global Venue Selection Factors

i. Factor 1—The Market

The United States has a gross domestic product (GDP) of $27.36 trillion and a population of approximately 334 million.[17] It is the largest consumer market in the world, and it is one of the most dominant markets for many of the technologies that are most often implicated in patent litigation matters. The U.S. represents, for example, on the order of 40 percent of the global markets in medical devices, pharmaceuticals, and software and information technology.[18] It represents about one-quarter of the market for global telecommunications services.[19] It is the second largest market for automotive vehicle sales, representing about 22 percent of the worldwide total, and was the second-largest

16. America Invents Act of 2011, Pub. L. No. 112-29, 125 Stat. 284 (2011), https://www.congress.gov/bill/112th-congress/house-bill/1249. The post-grant proceedings created under the AIA include inter parties review and also the less-commonly used post-grant review and covered-business-method review. For an overview of the USPTO PTAB post-grant proceedings, *see Sedona Parallel USPTO Proceedings*, *supra* note 3.

17. *See United States*, THE WORLD BANK, https://data.worldbank.org/country/united-states?view=chart (last visited Nov. 7, 2024).

18. *See Software and Information Technology Industry*, SELECTUSA, https://www.trade.gov/selectusa-software-and-information-technology-industry (last visited Nov. 7, 2024); *see also Global Pharma Spending Will Hit $1.5 Trillion in 2023, says IQVIA*, PHARMACEUTICAL COMMERCE (Jan. 29, 2019), https://www.pharmaceuticalcommerce.com/view/global-pharma-spending-will-hit-1-5-trillion-in-2023-says-iqvia.

19. *See Global telecommunications services market value from 2012 to 2019, by region*, STATISTA, https://www.statista.com/statistics/268636/telecommunications-services-revenue-since-2005-by-region/(last visited Nov. 7, 2024).

car manufacturer in 2023, with a 12 percent global market share.[20]

ii. Factor 2—The Quality of Adjudication

As one of the longstanding, predominant venues for patent litigation, the U.S. has a well-articulated and well-understood system for adjudicating patent disputes. U.S. laws relating to the public's access to the courts assure a high degree of transparency in U.S. patent proceedings, and the sophistication of the systems for capturing, retaining, and retrieving U.S. court records has made it possible for those interested in patent litigation to access most of the court filings online, including databases that are capable of generating an extraordinarily comprehensive range of statistical information about the performance of and outcomes in most U.S. federal courts.

The U.S. Court of Appeals for the Federal Circuit was created in 1982 as the sole national court of review for patent cases (along with certain other civil cases and administrative rulings) to develop a uniform nationwide body of law for patent matters and foster the development of a corps of appellate judges with deep expertise in patent matters.

By comparison, U.S. federal district courts of first instance are courts of general jurisdiction, with patent matters comprising only one of a wide variety of matters on their dockets. However, a number of factors—including U.S. venue

---

20. *See* Amaka Anagor-Ewuzie, *10 World's Biggest Automobile Producing Countries in 2023*, Business Day (April 23, 2024) and *Motor Vehicle Production Volume Worldwide in 2023, by Country*, STATISTA, https://www.statista.com/statistics/584968/leading-car-manufacturing-countries-worldwide/. (Last visited May 15, 2024), David Gorton, *6 Countries That Produce The Most Cars*, INVESTOPEDIA (Dec. 8, 2021), https://www.investopedia.com/articles/markets-economy/090616/6-countries-produce-most-cars.asp#toc-2-united-states-of-america.(last visited May 15, 2024).

rules, expedited schedules (trial by jury in perhaps as little of 12 months), predictable rules applicable to patent cases, the incorporation of many companies in Delaware, the strategic market locations for tech companies, and/or the opportunity for significant damages awards, enhancement of those damages, and injunctive remedies—have resulted in a very high concentration of patent lawsuits in the technology space in a small number of jurisdictions and judges, primarily in the Western District of Texas, the Eastern District of Texas, the District of Delaware, the Northern District of California, and the Central District of California.[21] In the pharmaceutical space, a concentration of patent lawsuits are filed in the District of New Jersey and the District of Delaware. As a result of this concentration, these federal district courts have a great deal of sophistication in patent law, the difficult art of managing patent cases, and the core patent litigation technologies.

iii. Factor 3—Time to Trial and Final Relief

Time to trial varies substantially based on the forum where the lawsuit is brought. A study on the average time to claim construction and trial highlights the discrepancies between judges and forum, and how this factor may strategically weigh in favor of a particular forum. For example, of five of the most popular courts in 2023, the Western District of Texas court's average time to claim construction was approximately 15 months, followed by the Eastern District of Texas at 17 months, the Central District of California at 21 months, the District of Delaware at 26 months and lastly, the Northern District of Illinois at 39 months..[22] In regard to the average time to jury trial

21. *See* DOCKETNAVIGATOR, OMNIBUS REPORT.

22. *See* IAM, Docket Navigator and IAM Litigation Report Q4 2023: Patent Litigation Special Report (Feb. 14, 2024), https://www.iam-media.com/

in 2023, the Western District of Texas court averaged 29 months, the Eastern District of Texas court averaged 31 months, the Central District of California averaged 36 months, the District of Delaware averaged 45 months, and the Northern District of Illinois averaged 49 months.[23]

The average time to bench trial in 2023 averaged 23 months in the Western District of Texas, 40 months in the Eastern District of Texas, 53 months in the Central District of California, 39 months in the District of Delaware, and 53 months in the Northern District. Overall, the Eastern and Western Districts of Texas provided the fastest timelines for resolution among the most popular courts.[24] The quicker pace of litigation in these jurisdictions may be particularly useful to parties who are trying to understand the merits of the case early on so that they can settle before expensive and lengthy discovery, and well before trial.

The median time to trial on patent infringement among all federal district courts for cases that reached trial in 2023 was 41 months for jury trial and 50 months for bench trials.[25] The Western District of Texas had the fastest average time to trial.[26]

Time to final relief in cases that proceed to trial (as opposed to cases that are resolved prior to trial) is significantly affected by time to trial itself but is also typically extended because of posttrial briefing and because certain relief, such as injunctive relief, is awarded by the judge after the completion of a jury trial. Final relief may also be delayed pending appeal.

---

data/docket-navigator-iam-litigation-report/2023-q4/article/docket-navigator-and-iam-litigation-report-q4-2023.

23. *Id.*
24. *Id*.
25. *Id*.
26. *Id*.

Apart from the federal district courts, the other main venue for resolution of patent disputes, provided the jurisdictional requirements are met, is the USITC. This is one of the fastest venues in the country, with a median time of nine months for a claim construction ruling and median time of 7.7 months to obtain an initial determination after a hearing before an administrative law judge. Overall, while the USITC is not authorized to award monetary damages, the USITC provides relatively fast resolution, can lead to a stay of a parallel federal district court case at the defendant**'s** option, and can greatly assist the parties toward timely concluding settlement negotiations to resolve patent-related disputes.

iv. Factor 4—Likelihood of Prevailing on the Merits

For federal district court cases resolved between 2018 and 2023, 7 percent resulted in a judgment on the merits (i.e., default judgment, consent judgment, judgment on the pleadings, summary judgment, trial, or judgment as a matter of law) in favor of the patent holder, whereas the defendant won about 3 percent of the time.[27] The vast majority of cases settled or ended as a result of some procedural resolution (i.e., dismissal, stay, multidistrict litigation, etc.). The likelihood of the patent holder prevailing in cases that go to a resolution on the merits (i.e., patents are valid, infringed, and enforceable) has been roughly 40 percent in recent years, [28] a success rate that varies

27. LEX MACHINA, FEDERAL DISTRICT COURT, CASES TERMINATED BETWEEN 1/1/2018 AND 12/31/2023 (last visited May 13, 2024).

28. IAM, Docketnavigator and IAM Litigation Report Q4 2023: Patent Litigation Special Report, https://www.iam-media.com/data/docket-navigator-iam-litigation-report/2023-q4/article/docket-navigator-and-iam-litigation-report-q4-2023, at 6. But *compare* John R. Allison and Mark A. Lemley, *Understanding the Realities of Modern Patent Litigation*, 92 TEX. L. REV.

significantly depending on the district court in which the action is brought.

At the USITC, the likelihood of the patent holder (i.e., the Complainant) prevailing on the merits in a Section 337 investigation averaged about 21 percent during the period of October 2016 through the end of 2021.[29] Of 262 cases, 87 were settled, the patent challenger won 94 times, the patentee won 37, and 44 resulted in a mixed outcome. In 2023, the USITC found a Section 337 violation in 13 of 26 investigations (50 percent).[30]

U.S. Supreme Court and Federal Circuit case law interpreting 35 U.S.C. § 101 has had a significant impact on the patentability of software and of medical diagnostic methods and related technology. In *Alice Corp. v. CLS Bank International*, which involved a Section 101 challenge to the patentability of business-method software claims, the Supreme Court noted that "merely requiring generic computer implementation fails to transform [an] abstract idea into a patent-eligible invention."[31] Since the Supreme Court's decision in *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, patents related to medical diagnostic methods have been difficult to obtain and enforce.[32]

1769 (2014) (reporting 26 percent overall patentee win rate in cases with dispositive rulings for all patent cases filed in 2008-09).

29. DOCKETNAVIGATOR, 2021 YEAR IN REVIEW: SPECIAL REPORTS, https://brochure.docketnavigator.com/2021-year-in-review/ at 37 (last visited May 14, 2024).

30. *Section 337 Statistics: Number Cases in Which Violation is Found/YR* (Updated Oct. 12, 2023), U.S. INT'L TRADE COMM'N, https://www.usitc.gov/intellectual_property/337_statistics_number_cases_which_violation.htm.

31. Alice Corp. v. CLS Bank Int'l, 573 U.S. 208, 212 (2014).

32. Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66, 70 (2012).

v. Factor 5—Availability of Effective Relief

Injunctive Relief. In the U.S., a patent owner may seek permanent injunctive relief barring the sale, use, or manufacture of a product or service following a trial court judgment that the patent is valid and infringed (35 U.S.C. § 283). The party seeking injunctive relief must show (1) it has suffered irreparable injury, (2) monetary damages are inadequate, (3) that considering the balance of hardships, an injunction is warranted, and (4) the public interest would not be disserved by a permanent injunction.[33] A number of studies have found that prevailing patent owners secure permanent injunctive relief between 80 and 90 percent of the time.[34] It should be noted that the competitive posture of the party seeking injunctive relief has a dramatic impact on its availability. One study estimates that injunctive relief is successfully procured only 16 percent of the time where the patent owner is a "patent assertion entity," but 80 percent of the time for all other plaintiffs, and 84 percent of the time in competitor v. competitor lawsuits.[35]

Of the 1,118 preliminary injunctions requested between 2009 and 2024 in U.S. federal district court patent matters, only 631 (56 percent) were granted.[36]

An alternative source of injunctive-type relief is the USITC. The USITC has the ability to bar importation of goods into the United States where the imports are shown to be

33. eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388, 391 (2006).

34. LEX MACHINA, FEDERAL COURTS DATABASE, REMEDIES (last visited May 14, 2024) (finding an average of 84 percent for the period 2009-24). Christopher B. Seaman, *Permanent Injunctions in Patent Litigation After eBay: An Empirical Study*, 101 IOWA L. REV. 1949, 1969 (2016) (collecting data from published sources); *see also, id.* at 1983 (finding that the permanent injunction grant rate for the period from May 2006 to December 2013 was 72.5 percent).

35. Seaman, *supra* note 344, at 1988, 1990.

36. LEX MACHINA, *supra* note 34.

anticompetitive for a variety of reasons. One basis for barring imports is a determination that the imported goods infringe a valid U.S. patent, where it is shown that the importation of the infringing goods would injure a domestic U.S. industry that lawfully practices the patent. The USITC does not have the authority to award monetary relief, but orders barring importation are routinely awarded to prevailing plaintiffs and enforced at the border by the U.S. Customs Service.

Substantial Damages. The U.S. Patent Act mandates that a prevailing patent owner "shall be awarded damages adequate to compensate for the infringement, but in no event less than a reasonable royalty for the use made of the invention by the infringer." [37] In "egregious" cases, a court may "increase damages up to three times the amount found."[38]

Between 2009 and 2024, damages were awarded in 701 patent cases in the aggregate amount of $19.7 billion.[39] Damages were enhanced just above 25 percent of the time. [40] The breakdown by type of award and the average award per case are summarized in the following table:[41]

37. 35 U.S.C. § 284.

38. *Id.*, *See* Halo Elecs., Inc. v. Pulse Elecs., Inc., 579 U.S. 93 (2016) (establishing the "egregiousness" standard for willful infringement determinations); SRI Int'l, Inc. v. Cisco Sys., 14 F.4th 1323, 1330 (Fed. Cir. 2021). For full discussion, *see* The Sedona Conference, *Commentary on Patent Litigation Best Practices: Willful Infringement Chapter*, Public Comment Version (July 2020) https://thesedonaconference.org/publication/Commentary_on_Patent_Litigation_Best_Practices_Willful_Infringement_Chapter.

39. LEX MACHINA, FEDERAL COURTS DATABASE, DAMAGES (last visited May 14, 2024).

40. *Id.*

41. *Id.*

	Number	Aggregate Amount	Mean Amount
All cases 2009-2024	701	$19.7 billion	$28.2 million
Reasonable Royalty	542	$14.8 billion	$27.4 million
Lost Profits	211	$3 billion	$14.3 million
Enhanced Damages	177	$1.8 billion	$10.6 million

Juries in some U.S. districts are perceived as being more inclined to award high patent damages awards than others, which can be a factor in patent venue selection.

vi. Factor 6—Cost of Litigation

The median cost of U.S. patent litigation is set forth in the chart below.[42]

Median Litigation Costs		
Year	**Discovery, motions, and claim construction**	**Pre- and post-trial and appeal when applicable**
Less than $1 million at risk		
2014	$400,000	$600,000
2016	$250,000	$500,000
2018	$250,000	$700,000
2020	$300,000	$675,000
2022	$300,000	$600,000

42. AM. INTELLECTUAL PROP. L. ASS'N, 2023 AIPLA REPORT OF THE ECONOMIC SURVEY (2023), https://www.aipla.org/home/news-publications/economic-survey/2023-report-of-the-economic-survey.

Median Litigation Costs		
Year	**Discovery, motions, and claim construction**	**Pre- and post-trial and appeal when applicable**
$1-10 million at risk		
2014	$950,000	$2 million
2016	$550,000	$1 million
2018	$600,000	$1.5 million
2020	$650,000	$1 million
2022	$600,000	$1 million
$10-25 million at risk		
2014	$1.9 million	$3.1 million
2016	$1 million	$2 million
2018	$1.2 million	$2.7 million
2020	$1 million	$3 million
2022	$1.5 million	$3 million
More than $25 million at risk		
2014	$3 million	$5 million
2016	$1.7 million	$3 million
2018	$2.4 million	$4 million
2020	$2.1 million	$4 million
2022	$1.5 million	$3.6 million

As can be seen, typical litigation costs (including both legal fees and other expenses) through trial in the U.S. range from roughly $1 million to more than $6 million depending on the size of the case. In the most complex and highly contested matters, it is more common for the total costs to reach into the tens of millions of dollars. It is also more common to see more expensive litigation costs in USITC cases given the rapid nature

of proceedings.[43] Notably, costs usually double (or more) if a case proceeds all the way through trial. In a change from previous years, the costs in suits brought by nonpracticing entities (NPEs) are slightly higher.[44]

vii. Factor 7—Recovery of Fees

Generally, attorneys' fees are not recoverable in patent suits unless the prevailing party can show an "exceptional case."[45] A case is exceptional if it "stands out from others with respect to the substantive strength of a party's litigating position (considering both the governing law and the facts of the case) or the unreasonable manner in which the case was litigated."[46] There "is no precise formula" for making this determination, but courts consider a number of factors, including "frivolousness, motivation, objective unreasonableness . . . and the need in particular circumstances to advance considerations of compensation and deterrence."[47] The exceptional-case determination is committed to the discretion of the district court and is evaluated on a case-by-case basis.[48]

---

43. *Id.* at 62. For example, a case with $1 million to $10 million at risk averages $2 million for discovery, motions, and claim construction, and around $4 million for a case that goes through trial at the USITC.

44. *Id.* at 61.

45. 35 U.S.C. § 285.

46. Octane Fitness, LLC v. ICON Health & Fitness, Inc., 572 U.S. 545, 554 (2014).

47. *Id.* at 554 & n.6 (quotations omitted).

48. *See id.* at 554. For detailed discussion, *see* The Sedona Conference, *Commentary on Patent Litigation Best Practices: Section on Exceptional Case Determinations*, Public Comment Version (Oct. 2016), https://thesedonaconference.org/publication/Commentary_on_Patent_Litigation_Best_Practices_Case_Management_Issues_from_the_Judicial_Perspective.

In 2023, attorneys' fees were awarded in 90 cases.[49] The average amount of those awards was approximately $406,355.[50]

b. Opportunity For Defendant-Initiated Litigation

An accused infringer can bring a suit seeking a declaration of noninfringement and invalidity (or any other available defense). A declaratory judgment action requires the parties to have an "actual controversy."[51] To determine whether there is an actual controversy, courts consider "whether the facts alleged, under all the circumstances, show that there is a substantial controversy, between parties having adverse legal interests, of sufficient immediacy and reality to warrant the issuance of a declaratory judgment."[52]

Conduct from which an intent to enforce a patent can be reasonably inferred can create declaratory judgment jurisdiction.[53] Although "a communication from a patent owner to another party, merely identifying its patent and the other party's product line, without more" will not support a declaratory judgment suit, showing additional facts to support a declaratory judgment is not difficult, especially when the

49. LEX MACHINA, FEDERAL COURTS DATABASE, DAMAGES (last visited May 24, 2024).

50. *See id*. The average award is heavily influenced by a large award in one case, which represented more than 50 percent of the aggregate award total for the 90 cases. Thus, the average award number overstates the award in a typical case.

51. MedImmune, Inc. v. Genentech, Inc., 549 U.S. 118, 126 (2007) (quotations omitted).

52. *Id.* at 127.

53. *See* Hewlett-Packard Co. v. Acceleron LLC, 587 F.3d 1358, 1363 (Fed. Cir. 2009).

patent owner is an NPE.[54] Accordingly, many patent owners (particularly NPEs) file suit before opening negotiations.

A declaratory judgment action does not change any of the substantive elements of an infringement case. Therefore, one of the primary purposes of a declaratory judgment suit is to select the forum for the litigation. But a demand letter, standing alone, is not sufficient to establish personal jurisdiction over a nonresident patent owner.[55] Nor is the presence in the forum of nonexclusive licensees of the patent owner.[56] In addition, a suit seeking a declaration of noninfringement or invalidity is governed by the general venue statute, not the patent venue statute.[57]

In selecting a preferred forum, parties consider the ability and willingness of the forum to protect its own jurisdiction. This most often manifests as an anti-suit injunction, which is a court order that prohibits the opposing party from pursuing litigation

---

54. *Id.* at 1362 (finding an implied threat of patent litigation by an NPE that stated that its patents "related" to Hewlett Packard's products and refused to enter into a 120-day standstill agreement).

55. *See* Red Wing Shoe Co. v. Hockerson-Halberstadt, Inc., 148 F.3d 1355, 1360–61 (Fed. Cir. 1998). Additional conduct, such as physically visiting the forum for licensing negotiations or filing other infringement suits in the forum, may be sufficient, however, especially for foreign NPEs. *See* Xilinx, Inc. v. Papst Licensing GmbH & Co. KG, 848 F.3d 1346, 1357–58 (Fed. Cir. 2017).

56. *See Red Wing*, 148 F.3d at 1361–62. But when a patent owner has an exclusive licensee or distributor in the forum, personal jurisdiction may be proper. *See* Breckenridge Pharm., Inc. v. Metabolite Labs., Inc., 444 F.3d 1356, 1366–67 (Fed. Cir. 2006).

57. *See* VE Holding Corp. v. Johnson Gas Appliance Co., 917 F.2d 1574, 1583 (Fed. Cir. 1990), *abrogated on other grounds by* TC Heartland LLC v. Kraft Foods Grp. Brands LLC, 137 S. Ct. 1514 (2017) ("It has long been held that a declaratory judgment action alleging that a patent is invalid and not infringed . . . is governed by the general venue statutes, not by § 1400(b).").

in a foreign court that has concurrent jurisdiction over the case. Relatedly, a party may seek an anti-interference injunction, also referred to as an anti-anti-suit injunction, whereby a party requests that the court order the opposing party not to further pursue or enforce an injunction from a foreign court that would interfere with the jurisdiction of the U.S. court or otherwise impair the party's ability to enforce its rights under U.S. law. While historically rare in the patent litigation context, there have been several recent instances of U.S. courts imposing injunctive relief to preserve the ability to pursue patent infringement actions in the U.S. and abroad.[58]

U.S. courts have also constrained patent owners' infringement claims through anti-suit injunctions and anti-anti-suit injunctions. In most circumstances there were overarching FRAND issues that could dispose of the entire action.[59]

---

58. *See* Ericsson Inc. v. Samsung Elecs. Co., Ltd., No. 2:20-cv-380, 2021 WL 89980 (E.D. Tex. Jan. 11, 2021) (imposing an anti-anti-suit injunction against the anti-suit injunction awarded by a Chinese court in a parallel proceeding); Continental Automotive Sys., Inc. v. Avanci, LLC, No. 19-cv-2520, Dkt. 187 (N.D. Cal. Oct. 8, 2019) (not granting a motion for an anti-suit injunction to prevent infringement proceedings brought by Nokia in Germany); Lenovo (United States) Inc. v. IPCom GmbH & Co. KG, No. 5:19-cv-1389, Dkt. 71 (N.D. Cal. Dec. 12, 2019) (terminating Lenovo's motion for an anti-suit injunction after a French court ordered Lenovo in a parallel proceeding to withdraw its motion for an anti-suit injunction).

59. *See* TCL Commc'n Tech. Holdings v. Telefonaktiebolaget LM Ericsson, No. 8:14-cv-341, 2015 U.S. Dist. LEXIS 191512 (C.D. Cal. June 29, 2015) (granting an anti-anti-suit injunction to prevent Ericsson from pursuing foreign patent claims on SEPs that were subject to the court's global FRAND determination); Huawei Techs. Co. v. Samsung Electronics Co., No. 3:16-cv-2787, 2018 WL 1784065 (N.D. Cal. Apr. 13, 2018) (granting an anti-anti-suit injunction against Huawei from enforcing injunction orders issued by a Chinese court); Microsoft Corp. v. Motorola, Inc., 696 F.3d 872 (9th Cir. 2012) (granting an anti-anti-suit injunction against Motorola from enforcing any injunction issued by a German court).

Another offensive option for accused U.S. infringers is to initiate an inter partes review (IPR) before the Patent Trial and Appeal Board (PTAB), the adjudicatory component of the U.S. Patent and Trademark Office.[60] Under this procedure, the defendant in a federal district court patent infringement action can seek review by the PTAB of the validity of the patents-in-suit. The board makes a threshold determination as to whether to "institute" the IPR by determining whether there is a "reasonable likelihood" that the petition will succeed in whole or in part. Depending on the scope of the relief sought in the IPR and whether it is instituted, a district court may stay the patent infringement case pending resolution of the IPR. This may take up to 18 months, and the stay may, in some instances, be extended up to an additional 12 months while the appellate court reviews the PTAB decision. If an IPR petition is not instituted, the case is litigated in full in the federal district court. If the IPR is instituted, the validity determination will resolve the issue for the federal district court proceeding insofar as it relates to the types of invalidity determinations within the purview of the PTAB—namely (for the most part) validity determinations based on printed publications and patents. However, in the relatively rare instances where the PTAB is considering a petition for post-grant review (not a petition for IPR), the board may also look at other validity issues, including, for example, those based on prior art products or services insofar as they were made public in the marketplace, and validity issues arising under Sections 101 (patentable subject

60. For a full discussion of IPR and other post-grant proceedings that can be filed before the USPTO Patent Trial and Appeal Board, *see Sedona Parallel USPTO Proceedings*, *supra* note 3.

matter) and 112 (enablement, written description, indefiniteness) of the Patent Act.[61]

Between 2014 and 2018, the number of IPRs filed was relatively steady at between 1,500 and 1,800 petitions a year. Since then, however, the number of IPR filings per year has been dropping. Between 2019 and 2023, the number of IPRs filed averaged 1,298 IPR petitions a year.[62] Of the instituted 2,243 IPRs that proceeded to trial between 2021 and 2023, 932 resulted in the invalidation of all claims at issue; 246 resulted in the affirmance of all claims at issue; and 233 resulted in mixed findings.[63] Other instituted IPRs were settled, joined to other trials, procedurally dismissed or disclaimed by the patent owner.

c. Current Developments in Patent Litigation in the U.S.

While many favored patent jurisdictions have become more congested over the last few years for a variety of reasons,[64] a court in the Western District of Texas is one of the fastest in the

61. While the PTAB routinely considers over 1,000 IPR petitions each year, post-grant review petitions are rarely filed. For example, in the period from Oct. 1, 2022 to Sept. 30, 2023, only 30 PGR petitions were filed, compared to 1,209 IPR petitions in the same period. *See* USPTO Patent Trial and Appeal Board, *PTAB Trial Statistics, FY23 End of Year Outcome Roundup IPR, PGR*, https://www.uspto.gov/sites/default/files/documents/ptab_aia_fy2023__roundup.pdf.

62. LEX MACHINA, PATENT TRIAL AND APPEAL BOARD, SUMMARY OF IPR FILINGS (last visited May 15, 2024). LEX MACHINA, PATENT LITIGATION REPORT (Feb. 2024), at 25.

63. *Id.* at 30.

64. United States Courts, U.S. District Courts-Combined Civil and Criminal Federal Court Management Statistics (Dec. 31, 2023), https://www.uscourts.gov/statistics/table/na/federal-court-management-statistics/2023/12/31-3.

country for patent litigation. In this court's Standing Order Governing Proceedings for Patent Cases, issued October 8, 2021, trials are scheduled to conclude within eighteen months.[65] In some situations, case management schedules in the Western and Eastern Districts of Texas can provide for matters to be concluded in as little as 12 months.

An expedited procedural schedule is an important consideration for patent owners seeking a quick resolution as well as to head off potential institution of an IPR by the PTAB. This is because the PTAB looks at certain factors, known as the "*Fintiv* factors," when considering whether to institute an IPR when litigation is copending: whether the court will grant a stay, the proximity of the trial date, an overlap of issues between the district court and IPR, the investment in the district court proceedings, whether the parties are the same, and any other circumstance that would impact the board's exercise of discretion. Between 2021 and 2023, the PTAB denied 439 petitions on procedural grounds, roughly 11 percent of all institution decisions, relying on the *Fintiv* factors and the "trial date" framework for 51 percent of all denials under 35 U.S.C. 314(a).[66] As a result, patent owners are even more motivated to file their patent litigation complaints in forums that provide a fast trial schedule.

---

65. Judge Alan D. Albright, Standing Order Governing Proceedings-Patent Cases (Apr. 4, 2023), https://www.txwd.uscourts.gov/wp-content/uploads/2023/01/Standing-Order-Governing-Patent-Cases.pdf.

66. LEX MACHINA, PATENT LITIGATION REPORT (Feb. 2024), at 30. *See PTAB Uses Discretion, Fintiv to Deny Petitions 38% in 2021 to Date* (Sept. 22, 2021), UNIFIED PATENTS, https://www.unifiedpatents.com/insights/2021/9/22/an-early-look-at-the-ptabs-use-of-fintiv-and-discretion-discretionary-denials-through-september-2021; *PTAB Discretionary Denials Up 60%+ in 2020: Fueled Entirely by 314(a) Denials* (Jan. 5, 2021), UNIFIED PATENTS, https://www.unifiedpatents.com/insights/2020-ptab-discretionary-denials-report.

2. Brazil

Brazil can be an attractive venue for patent owners to file infringement actions and to obtain preliminary injunctions, subject to a relatively expedited interlocutory appeal. A party would need to establish a likelihood of eventually prevailing on the merits and that the party will be harmed in the absence of such injunctive relief. Technical evidence showing likelihood of infringement is needed for patent owners to obtain a preliminary injunction. In addition, injunctive relief may be granted before any consideration of validity under the bifurcated court system in Brazil.

a. Global Venue Selection Factors

i. Factor 1—The Market

Brazil is the ninth largest economy in the world and the largest in Latin America,[67] with a population of approximately 216 million. [68] In 2019, Brazil signed a significant trade agreement with the European Union after twenty years of negotiation.[69]

In July 2019, the Brazilian Ministry of Economy and the Brazilian Patent Office (BRPTO) announced a plan to tackle

67. *See* U.S. Dep't of State, 2021 Investment Climate Statements: Brazil, https://www.state.gov/reports/2021-investment-climate-statements/brazil/ (last visited Nov. 7, 2024).

68. *See Brazil*, THE WORLD BANK, https://data.worldbank.org/country/brazil (last visited Nov. 7, 2024).

69. *See* European Commission Press Release, EU and Mercosur reach agreement on trade (June 27, 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_3396; *see also* Amandine Van Den Berghe, *What's Going On with the EU-Mercosur Agreement?*, CLIENT EARTH (June 11, 2021), https://www.clientearth.org/latest/latest-updates/news/what-s-going-on-with-the-eu-mercosur-agreement/.

patent examination pendency.[70] By March 2022, according to BRPTO's official data, this plan resulted in a reduction of 79.57 percent of patent applications pending for decision.[71]

ii. Factor 2—The Quality of Adjudication

Brazil is a civil law country but implements a bifurcated court system that operates on the state and federal levels. For instance, patent infringement actions are filed before the state courts. Some states, such as São Paulo and Rio de Janeiro, have district courts specialized in commercial disputes, including patent litigation matters. São Paulo and Rio de Janeiro are the largest patent litigation venues in Brazil, with São Paulo also having specialized chambers at the appellate level.

There is no discovery phase in Brazil. After the pleading phase, parties submit evidence production requests to the court. The court then issues a case management decision, establishing the controversial points that require further evidence production to be solved, and grants the parties' evidence requests that are deemed relevant to solve such controversial issues.

It is possible (as in the French system) to seek a search at the defendant's premises, allowing the patentee together with a Brazilian public officer to enter the premises of the defendant and to describe the accused product or process in a report, as well as seize samples of the accused products. This measure, however, is considered more extreme and is rarely conducted.

---

70. *See Bye, bye backlog? Government measures to stimulate business in Brazil*, LICKS ATTORNEYS (July 10, 2019), https://www.lickslegal.com/news/bye-bye-backlog-government-measures-to-stimulate-business-in-brazil.

71. *See* Kene Gallois, *Brazil's Patent System: Latest Statistics on Efforts to Reduce the Backlog and the Road Ahead*, IPWATCHDOG (July 1, 2021), https://ipwatchdog.com/2021/07/01/brazils-patent-system-latest-statistics-efforts-reduce-backlog-road-ahead/.

Parties can use technical experts. Courts can also appoint an unaffiliated expert to provide written opinions addressing infringement or validity. There is no examination or cross-examination of experts.

Although invalidity arguments may be raised in patent infringement actions before the state courts as a matter of defense, invalidity cases in Brazil can only be filed before the federal courts.[72] Federal courts in Rio de Janeiro have specialized district and appellate courts to hear IP validity cases. Notably, in a validity lawsuit, the Brazilian Patent and Trademark Office is a codefendant with the patent owner.

iii. Factor 3—Time to Trial and Final Relief

Disputes usually last between two and four years at the trial court of first instance, depending on the court's productivity and the parties' involvement. Infringement proceedings start when a patent owner files a lawsuit before a state court. Regarding the validity of a challenged patent, the challenger can file an invalidity lawsuit against the patent owner and the BRPTO before a federal district court at any time during the patent term. In addition, the Brazilian Patent Statute provides the possibility of a post-grant opposition procedure.[73] The post-grant opposition can be filed by the BRPTO or by a third party until six months after the grant of the patent.

---

72. *See* Law No. 9,279/96 [Brazilian Patent Statute], Art. 56; *see also* Andre Venturini et al., *Global patent prosecution 2022 - Brazil*, IAM (Oct. 28, 2021), https://www.lexology.com/library/detail.aspx?g=175496a3-792e-4f08-86ac-2369f4f99d6b.

73. Brazilian Patent Statute, *supra* note 72, Art. 51.

iv. Factor 4—Likelihood of Prevailing on the Merits

Brazil has a relatively positive environment for patent holders. Preliminary injunctions on patent infringement cases are statutorily allowed.[74] It is also possible to obtain exclusion orders against the importation of infringing products. Additional remedies include search and seizure of goods, accounting documents, and a daily penalty against patent infringers. In view of the strong remedies available, there is a high rate of settlements before trial.

In addition, the courts are known as not displaying a significant bias between nonpracticing entities and practicing entities.

v. Factor 5—Availability of Effective Relief

Preliminary injunctions are available and often requested by plaintiffs in infringement lawsuits. The requirements for the granting of a preliminary injunction are (i) strong evidence that convinces the judge of the likelihood of the plaintiff's claims, and (ii) risk of irreparable harm.

Pharmaceutical litigation is growing in Brazil, and preliminary injunctions are available regardless of whether a patent holder is seeking to enforce compound claims or use claims. Preliminary injunctions are also available for process claims, albeit requiring a higher threshold to be met with the prima facie evidence, due to the asymmetry of information between the parties, as processes are usually not public knowledge.

Damages can be sought in patent infringement proceedings. Awards will be determined on the basis of the counterfactual

74. *Id.*, Art. 209.

that the violation had not occurred.[75] Loss of profits will be determined by the most favorable, to the injured party, of the following criteria: (i) the benefits that would have been gained by the injured party if the violation had not occurred; (ii) the benefits gained by the author of the violation of the rights; or (iii) the remuneration that the author of the violation would have paid to the proprietor of the violated rights for a license that would have legally permitted him to exploit the subject of the rights.[76]

vi. Factor 6—Cost of Litigation

There is no discovery in Brazil. The typical litigation costs (including legal fees and other expenses) through trial in Brazil range from roughly $300,000 to more than $2 million, depending on the size and complexity of the case. However, costs increase when the parties seek to obtain preliminary and permanent injunctions.

vii. Factor 7—Recovery of Fees

Typically, the winner is entitled to receive court fees and other expenses incurred during the case, including the court-appointed expert's fees.[77] However, attorneys' fees are not reimbursed by the losing party.[78]

b. Opportunity For Defendant-Initiated Litigation

An accused infringer can file declaratory judgment suits seeking a declaration of noninfringement and invalidity. The

75. *Id.*, Art. 208.

76. *Id.*, Art. 210.

77. *Patent Litigation 2024-Brazil*, CHAMBERS AND PARTNERS (Updated Feb. 15, 2024), https://practiceguides.chambers.com/practice-guides/patent-litigation-2024/brazil.

78. *Id.*

standing requirement for a declaratory judgment of noninfringement in Brazil is low because the potential defendant only needs to show simple evidence of the likelihood that the patent is going to be asserted. For instance, evidence showing the behavior of the patent owner in similar circumstances can be enough evidence to support a noninfringement suit. One of the main purposes of a declaratory judgment suit is to enable the defendant to choose Brazil as a venue.

In addition, the Brazilian Patent Statute regulates post-grant review proceedings; any third party with a legitimate interest or the BRPTO can challenge a patent within six months from the grant. If the challenge is successful, the patent is invalidated with retroactive effect to the date of filing.

Parties can always consider an invalidity lawsuit or a declaratory validity lawsuit. Brazilian federal courts will hear such cases even when post-grant review proceedings are pending before the BRPTO.

c. Current Developments in Patent Litigation in Brazil

The most relevant recent development in Brazil was the Brazilian Supreme Court's declaration of unconstitutionality of the patent term that assured a 10-year minimum term from the grant date. The Court's 2021 ruling established a patent term of 20 years from the filing date.[79]

79. Direct Action of Unconstitutionality (ADI) 5,529 (Brazil Supreme Federal Court 2021), *available at* https://jurisprudencia.stf.jus.br/pages/search/sjur451892/false. *See* Roberto Rodrigues & Ana Calil, *Brazilian Supreme Court considers ruling on patent case for the first time this century*, J. OF INTELL. PROP. L. & PRAC., Vol. 16, No. 2 (Apr. 8, 2021) 146–49, https://doi.org/10.1093/jiplp/jpaa195.

The Supreme Court also ruled that the decision would have a retroactive effect for patents related to pharma products and methods, as well as medical equipment and supplies.[80] Patent owners and applicants with granted patents in the pharma and human health sectors will likely see an impact related to their license agreements and assets. The BRPTO has already issued the new patent terms for most of the affected patents.[81]

Patent owners have sought from the courts compensation for the delays during the patent's examination. Preliminary injunctions have been granted in some cases to keep in force patents that would otherwise already have expired under the base 20-year term, at least until judgment is rendered at the trial level.[82]

B. Europe

1. Germany

One of the key reasons to file a patent litigation suit enforcing a global patent portfolio in Germany is the availability of injunctive relief within roughly a year of litigation at moderate cost. Germany has a bifurcated system for patent cases in which infringement and invalidity are determined in separate proceedings by separate courts, resulting in the so-called "injunction gap" that is considered attractive by plaintiffs. Infringement proceedings are decided much more quickly than validity proceedings, and an injunction ordered by the infringement court of first instance can be provisionally

80. *Id.*

81. *Id.*

82. Rob Rodrigues et al., *Patent Term Adjustment in Brazil at the centre of major battle for IP owners*, IAM (May 30, 2023), https://www.iam-media.com/article/patent-term-adjustment-in-brazil-the-centre-of-major-battle-ip-owners.

enforced even if an appeal is filed and there is not yet a validity decision. Also attractive to patent plaintiffs is the fact that Germany has highly specialized patent courts and attorneys with a wealth of experience, leading to significant predictability and high-quality decisions, i.e., decisions that are respected, and often followed, in the rest of Europe.

Potential infringers often file proactive invalidity actions in Germany in anticipation of becoming a target of a future infringement suit.

a. Global Venue Selection Factors

i. Factor 1—The Market

Germany is the largest economy in Europe and fourth largest worldwide behind the U.S., China, and Japan (GDP is at approximately $4.45 trillion U.S.; GDP per capita is approximately $52,745 U.S.).[83] Germany is the third largest exporter worldwide.[84] Research and development accounts for 3.1 percent of Germany**'s** GDP.[85]

Significant portions of worldwide supply chains are often located within Germany. Twenty-eight of the world**'s** 500 largest stock-market-listed companies are headquartered in Germany, which also has a relatively large number of small and medium enterprises that are often market leaders in their specific segment.

---

83. *GDP (current US$)*, THE WORLD BANK, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?name_desc=false (last visited Nov. 7, 2024).

84. *Exports by Country 2024*, WORLD POPULATION REVIEW, https://worldpopulationreview.com/country-rankings/exports-by-country (last visited Nov. 7, 2024).

85. *Research and development expenditure*, THE WORLD BANK, https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS.

Hence, evidence of infringement is usually available, since the allegedly infringing products are quite often manufactured, distributed, and sold within Germany.

ii. Factor 2—The Quality of Adjudication

Generally, Germany has a high quality of adjudication due to the following factors: strong reputation (constitutional independence; specialist courts, judges, and lawyers; significant experience from adjudicating the highest number of cases by far in Europe year by year), predictable judgments (usually patentee-friendly), and a significant influence on other jurisdictions (e.g., the UK Supreme Court**'s** strong convergence to Germany**'s** approach to equivalence[86]). The latter aspect is particularly noteworthy, as German judgments often serve as pilot judgments for a European-wide or even global settlement.

The German courts' **"**injunction gap**"** significantly impacts the quality of the adjudication in favor of the plaintiffs and to the detriment of defendants. This injunction gap refers to the fact that injunctive relief can be imposed before any finding is made on patent validity in Germany, because:

- infringement and nullity (i.e., validity) are determined in separate proceedings by separate courts;
- infringement proceedings are decided much quicker than validity proceedings; and
- an injunction ordered by the infringement court of first instance can be provisionally enforced even if an appeal is filed and there is not yet a validity decision.

86. *See* Actavis v. Eli Lilly, UKSC 48 (UK Supreme Court 2017) (discussing the German court's approach to equivalents at length), *available at* http://www.bailii.org/uk/cases/UKSC/2017/48.html.

Regional courts are competent to hear infringement actions, but these courts do not have jurisdiction to determine the validity of a patent-in-suit. For an invalidity determination, the defendant has to lodge an opposition with the European Patent Office (EPO) or—after lapse of the opposition period or a final decision by the EPO—file a nullity action with the German Federal Patent Court. The infringement courts only assess validity on a prima facie basis in order to decide whether to stay the proceedings. As a consequence and because the infringement proceedings move more rapidly than nullity actions, there is often a "gap" between the time that an injunction is issued by the regional court and the time when an invalidity determination is made.

The best that a defendant can achieve on the infringement side is a stay of the infringement proceedings in view of validity concerns. In practice, however, the grant of a stay is rare because the threshold—a "high likelihood of invalidation"—is high.[87]

German law, including its implementation of the Intellectual Property Rights Enforcement Directive of the European Union,[88] provides litigants with several options to retrieve evidence in the domain of the opposing party (or an unrelated third party). Regarding discovery and inspection, these mechanisms are available if the claimant can show a likelihood of infringement (which in practice is a somewhat higher hurdle

87. The rate to stay infringement proceedings pending the parallel validity proceedings has increased in recent years (based on the observation of those who actively practice in this area) from approximately 10 percent to 20-30 percent.

88. Directive 2004/48/EC of the European Parliament and of the Council of the European Union of 29 April 2004 on the enforcement of intellectual property rights [hereinafter EU Enforcement Directive], *available at* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:157:0045:0086:EN:PDF; German Act on Improvement of Intellectual Property Rights, Sept. 1, 2008, BGBL (implementing the EU Enforcement Directive).

than in other countries, e.g., France). However, the claimant has to specify exactly which documents have to be disclosed or where and what needs to be inspected. Furthermore, the claimant also needs to state why the disclosure of certain documents or the inspection of certain premises is important for the case and why there are no other reasonably available means to obtain the evidence sought. If an inspection request is successful, the claimants' outside counsel (counsel eyes only) and an expert are allowed to enter the premises of the defendant and describe the accused product or process in a report, seize samples of the accused products, and take copies of any documentation evidencing the materiality and also the origin and the scope of the infringement (including financial documentation, similar to France). Once performed, the defendant can file an appeal against the inspection order. If no appeal is filed or the appeal is unsuccessful, the report is released to the claimant and can then be used in litigation.

However, evidence is only necessary if a certain fact is contested by the other party, i.e., to the extent facts are actually in dispute between the parties. The level of substantiation to which a fact must be contested to be deemed inadmissible depends on the level of substantiation to which the other party supported that fact. Therefore, most factual disputes can be resolved without a need to take evidence by comprehensively presenting a respective fact, i.e., by very substantiated pleadings. In the context of seizures (of samples, documents, etc.) for infringement evidence purposes, preliminary measures (even ex parte) are available but rarely granted.

Generally, German court proceedings are public, and thus, there is no protection of confidential information by default. The parties, however, can request the court to exclude (i) the public during the oral hearing or (ii) certain parts of the file from a third-party file inspection request, but these measures are at the discretion of the court. In view of the implementation of the EU

Trade Secret Directive,[89] Germany has adopted various measures to protect confidential information in main proceedings. As a consequence of the recent German Patent Act reform,[90] these measures can now also be applied to patent infringement proceedings. For instance, the court may order the parties to not disclose certain protected information outside of the pending proceedings and limit the number of persons getting access to such information. Therefore, the presentation of proprietary technical information or of comparable license agreements under FRAND aspects is now considerably easier, and the protection of confidential information has been significantly improved.

German courts decide cases based on the legal briefs submitted by the parties, the exhibits filed, and the arguments made by the advocates during the court hearing, which usually lasts only a few hours. Cases are normally decided without live examination of experts or witnesses, but meaningful expert involvement is possible through written expert declarations and informal questioning by the court. Technical experts need not be local, and foreign experts are regularly relied upon.

A special advantage of patent litigation in German courts for plaintiffs is the availability of utility models that are registered within only a couple of weeks. This is particularly attractive for patent holders if they perceive an urgent need for a readily enforceable protective right. For instance, a utility model can be branched off from a still-pending patent application. Its claims can be tailored to the accused embodiment within the original disclosure of the parent patent application. In principle, utility models can be enforced in the same way as patents. However,

89. German Act on the Protection of Trade Secrets, Apr. 18, 2019, BGBL.

90. German Act on the Simplification and Modernization of German Patent Law, June 10, 2021.

the threshold for the defendant to achieve a stay is considerably lower since utility models are not substantively examined. Furthermore, unlike in patent infringement cases, an invalidity objection is available within the utility model infringement proceedings. Defendants, however, typically prefer to attack the validity of the utility model in separate cancellation proceedings and request the infringement court to stay the infringement proceedings until a decision on validity is available.

iii. Factor 3—Time to Trial and Final Relief

The time to trial depends on the chosen forum in Germany. Although the contributors to this *Framework* have not located any published data on this subject, the observations of those who actively practice German patent litigation are that time to trial is as follows:

- Federal Patent Court *only for nullity actions*: approximately 2.5 to 3 years.
- Regional Court Dusseldorf: approximately 12 to 18 months.
- Regional Court Mannheim: 8 to 12 months.
- Regional Court Munich I: approximately 12 months.
- Appellate Courts: approximately 1.5 to 2 years.

Final relief is available after the judgment has become legally binding. A first-instance judgment is preliminarily enforceable, but the winning party is required to deposit a security during the appeal period and the potentially lodged appeal. First-instance judgments are usually rendered a couple of weeks after the oral hearing. Second-instance judgments are also preliminarily enforceable *principally* without having to provide security (unless the losing party also provides security).

iv. Factor 4—Likelihood of Prevailing on the Merits

German courts are usually perceived as patentee-friendly, so there is—in general—a solid chance for patentees to prevail on the merits. Under the principle of submission and production of evidence, the claimant does not even have to fully prove its case. It might be sufficient to base its case on substantiated and concrete indications if the defendant is not able to contest these with the same level of substantiation.

v. Factor 5—Availability of Effective Relief

Preliminary Relief (i.e., preliminary injunctions and seizures). Preliminary relief is available, both in the form of injunctions as well as seizures.

Until recently, courts even issued ex parte injunctions, but due to recent case law by the German Constitutional Court, either the claimant (by way of warning letters or the like)[91] or the court has to ensure the defendant's right to be heard. Ex parte injunctions are still possible, but only in rare circumstances, e.g., in trade-fair matters.[92]

Injunctive Relief. Under German patent law, an injunction is issued if infringement is found (i.e., German courts issue so-called "quasi-automatic" injunctions). Since the reform of the German Patent Act in 2021, the claim for an injunction can be excluded or tailored in view of any disproportionate hardship for the defendant. However, that change in law merely codified

91. BVerfG, 1 BvR 1783/17 (Germany Federal Constitutional Court) Sept. 30, 2018, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2018/09/rk20180930_1bvr178317.html

92. BVerfG, 1 BvR 2421/17 (Germany Federal Constitutional Court) Sept. 30, 2018, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2018/09/rk20180930_1bvr242117.html.

the leading and very restrictive case law of the Federal Court of Justice (Germany**'s** highest court) so that an exclusion or tailoring of an injunction should only occur in exceptional and rare cases. Under an injunction, the defendant is ordered to cease and desist from, inter alia, manufacturing, offering for sale, distributing, and using the attacked product or process.

Other Relief. Other available relief includes recall and destruction of infringing products, public notification of the decision, the obligation to disclose details regarding suppliers and customers, and the obligation to disclose details regarding numbers and profits.

Substantive Damages. A first-instance judgment stipulates the defendant**'s** obligation to pay damages *in principle*. The actual amount is subject to a second proceeding. There, the claimant can freely choose from three options to calculate its damages: reasonable royalty, share of infringer**'s** profit, or own lost profits. Punitive damages are not available; only compensatory damages are available. Damages proceedings can be burdensome and time consuming. Very high damages awards are the exception rather than the rule. For this reason, in the majority of cases, the parties settle after any initial infringement decision (from a German or any internationally renowned court) and come to a commercially meaningful solution.

Border Detention Measures. The German customs authorities have become rather sophisticated (upon the request of IP proprietors) in detecting and detaining infringing products entering the European market via Germany. IP proprietors can request the cooperation of customs officials by filing a border detention request, listing the relevant IP rights and providing sufficient details for recognizing the goods upon arrival. When customs authorities encounter products that conform to a border detention request, they will normally retain the products and inform the IP proprietor forthwith, who can then follow up

with appropriate action (e.g., inspect and, if appropriate, initiate civil proceedings).

vi. Factor 6—Cost of Litigation

German litigation costs are significantly lower than U.S. or UK proceedings. The main driver for costs are the party**'s** own attorney fees (which are usually based on hourly rates). Depending on the complexity of the matter, such fees amount to approximately €100,000 to €250,000 for first-instance proceedings (infringement as well as nullity proceedings). Apart from that, the claimant has to advance the statutory court fees. Court-appointed experts are rare, so such costs are usually avoided. However, the fees can be higher in high-stakes cases, and recovery of fees is a relevant factor to be considered for the cost-risk analysis.

vii. Factor 7—Recovery of Fees

Germany has adopted a limited **"**winner-takes-all**"** principle. The winning party has a claim against the losing party for reimbursement of statutory attorney and court fees and other necessary expenses, such as travel and translation costs. The attorney and court fees are in turn based on the value in dispute, which depends on the patent holder's economic interest in winning the proceedings. For example, the reimbursable statutory fees for a value in dispute in the amount of €500,000 in first-instance infringement proceedings amount to approximately €16,000. Typical values in dispute range from €500,000 to €5 million. The statutory maximum value in litigation is €30 million.[93]

93. *See* [German] Federal Ministry of Justice, Lawyers' Remuneration Act – RVG, Annex 1 (to § 2 paragraph 2), Schedule of remuneration, *available at* https://www.gesetze-im-internet.de/rvg/anlage_1.html (last visited Nov. 7, 2024).

b. Opportunity For Defendant-Initiated Litigation

The only accepted opportunity to date for defendants to initiate litigation in Germany (besides bringing a proactive invalidity attack) is a negative declaratory action aimed at a judicial determination that the acts committed do not infringe the respective patent. For this, however, the potential defendant seeking the declaration needs to show a legal interest in this determination, which is usually established if the patentee has alleged that it has a claim for patent infringement against the claimant. A similar action could also be initiated, e.g., by way of an Italian or Belgian torpedo in other jurisdictions.[94]

Declarations of obviousness of a product over the state of the art on a particular date ("*Arrow* declarations")[95] and declarations of "FRAND-ness" of license offers in a standard-essential patent (SEP) dispute have not yet been decided by case law but are likely available in Germany, as in other European countries.

In SEP-FRAND cases, potential defendants can theoretically file a claim against the SEP holder based on the SEP holder's FRAND commitments. When ruling on the assertion by SEP defendants of such a "FRAND defense," a court need only decide whether the offer made by the patentee constitutes FRAND; it need not determine the scope of the FRAND conditions themselves. In adjudicating FRAND issues, the German courts stick closely to the requirements set out by the European Court of Justice in *Huawei v. ZTE*.[96] Accordingly, the defendant can raise a FRAND defense against the asserted

94. For discussion, *see supra* Sect. III.B (Delaying Proceedings).

95. For description of *Arrow* declarations, *see supra* note 11 and underlying commentary text.

96. Huawei Techs. Co. v. ZTE Corp., C-170/13 (CJEU 2015), *available at* https://curia.europa.eu/juris/liste.jsf?num=C-170/13.

claims for injunction, recall, and destruction. Even if the FRAND defense is successful, any claims for information, rendering of accounts, and damages are still enforceable, but any asserted claims for injunction, recall, and destruction may be limited to a FRAND royalty. The German SEP-FRAND case law is very much in flux and quite divergent between the practices of the Mannheim, Munich, and Dusseldorf courts in particular. To date, no German court has decided a specific FRAND royalty or range.

c. Current Developments in Patent Litigation in Germany

The most recent development in German patent litigation was a reform of the German Patent Act that took effect in August of 2021. The reform was lobbied for by the automotive and telecommunications industries and resulted in three important changes to the law. First, the claim for an injunction can be excluded or tailored in view of disproportionate hardship for the defendant. However, that change merely codified the leading and very restrictive case law of the Federal Court of Justice so that an exclusion of an injunction should only occur in exceptional and rare cases. Second, and much more importantly, a deadline of six months to provide a qualified written opinion on validity was imposed on the Federal Patent Court in nullity proceedings, in order to be used for stay requests on the infringement side. It remains to be seen whether the Federal Patent Court will be able to meet that requirement in reliable quality and whether the infringement courts will then follow the qualified written opinion. Third, the protection of trade secrets in patent infringement proceedings has been significantly improved by applying certain rules of the German Act on the Protection of Trade Secrets. For instance, the court may order the parties to not disclose certain protected information outside of the pending proceedings and limit the

number of persons getting access to such information (the "confidentiality club"). Therefore, the presentation of proprietary technical information or of comparable license agreements under FRAND aspects is now considerably easier.

2. United Kingdom

The United Kingdom is a common law jurisdiction with substantial discovery processes (albeit more limited than in the U.S.), oral evidence including cross-examination, and oral advocacy before specialist patents judges. This leads to decisions that are respected and often followed in Europe. Historically, it has attracted much international pharmaceutical litigation. More recently, there has been an influx of SEP-FRAND litigation owing to developments in the law.

a. Global Venue Selection Factors

i. Factor 1—The Market

The UK is presently the sixth largest economy in the world by GDP and the largest economy in Europe that is independent from the European Union. [97] It is also the 12th-ranked manufacturing country in the world.[98]

As such, it is a major market for pharmaceutical and electronic products that form the focus of much international patent litigation. Given the size of the market and the UK courts' liberal and compensatory approach to assessing damages,

97. *See* CENTRE FOR ECONOMICS AND BUSINESS RESEARCH (CEBR), WORLD ECONOMIC LEAGUE TABLE 2023 (Dec. 2022), https://cebr.com/wp-content/uploads/2022/12/WELT-2023.pdf.

98. *UK Manufacturing – The Facts 2024 report*, MAKE UK, https://www.makeuk.org/insights/publications/uk-manufacturing-the-facts-2024 (last visited Nov. 7, 2024).

awards for damages are relatively high compared with most jurisdictions around the world, other than the United States.

ii. Factor 2—The Quality of Adjudication

The United Kingdom comprises three civil jurisdictions: England and Wales, Scotland, and Northern Ireland (with the UK Supreme Court serving as the final court of appeal for all three jurisdictions). If an alleged infringing act takes place throughout the UK, then a claimant has a choice of jurisdiction. The territory of UK patents and European patents is UK-wide, and accordingly, the courts of any of the three constituent jurisdictions will grant injunctions that are UK-wide in scope. However, most patent litigation in the UK takes place in the Patents Court of England and Wales, which is the focus of the remainder of this section.

The Patents Court of England and Wales is widely regarded as very high quality. It is a specialist court within the Chancery Division of the High Court. As such, it has a bespoke procedure for patent cases and specialist judges. It deals with the higher value or more technologically complex cases in the UK; lower value or simpler cases are heard by another specialist IP court (the Intellectual Property Enterprise Court, which has special procedures aimed at reducing fees and costs, and with limited fee-shifting, discussed further below). All cases in the Patents Court are assigned to nominated patent judges, and those cases that have been assessed as more technically difficult (categories 4 and 5 on a scale of 1 to 5) are assigned to judges who are career patent lawyers. Historically, there have been two or three such career patent specialist judges. The patent judges are well respected by their peers in other jurisdictions and are influential in other jurisdictions that are members of the European Patent Convention, including Germany and the Netherlands. Judges in those jurisdictions will frequently follow UK judgments (and if they do not, will usually give reasons for differing).

English civil procedure allows for written disclosure or discovery (the degree of disclosure being tailored according to a flexible menu of options, but invariably less extensive than that in the United States), provision for conducting experiments, extended cross-examination of fact and expert witnesses, and oral proceedings before the judge.

iii. Factor 3—Time to Trial and Final Relief

In a statement dated February 1, 2022, the Patents Court confirmed that it endeavors to bring patent cases to a final liability trial where possible within 12 months of the claim being issued.[99] In practice, the time to liability trial is often longer, generally between 12 and 18 months.

It is possible for proceedings to be stayed pending European Patent Office opposition proceedings,[100] although this is not common and tends to happen only if the EPO opposition proceedings are well advanced.

Judgments will typically be handed down within a few weeks of trial, with the final order as to relief being made a month or so after that. In a case where a patent has been found valid and infringed, the order will set out the scope of any injunction ordered and also allow the commencement of a damages inquiry or an account of the infringer's profits (following the provision of limited disclosure to allow the

99. *See* Practice Statement: Listing of Cases for Trial in the Patents Court, [UK] COURTS AND TRIBUNALS JUDICIARY (Feb 1, 2022), https://www.judiciary.uk/guidance-and-resources/practice-statement-listing-of-cases-for-trial-in-the-patents-court/.

100. Virgin Atlantic Airways v. Zodiac Seats U.K., [2013] UKSC 46 (UK Supreme Court), *available at* https://www.supremecourt.uk/cases/uksc-2010-0013.html, and IPCom v. HTC Europe Co., [2013] EWCA (Civ.) 1496 (England and Wales Court of Appeal), *available at* https://www.bailii.org/ew/cases/EWCA/Civ/2013/1496.html.

successful patent holder to make an informed election between the two types of relief proceedings).

Permission is required to appeal a judgment and will not necessarily be granted, particularly if the judgment relates to questions of fact, or mixed questions of fact and law, such as obviousness or inventive step. If permission to appeal is granted, the appeal hearing will generally take place within about a year. The court will often stay any injunction pending appeal, balancing the interests of the parties if the judgment is overturned on appeal.[101] Usually, the court will require the patent holder to make a cross-undertaking to reimburse the defendant for its losses should the injunction be lifted on appeal.

As proceedings in the UK are bifurcated, the award of damages or infringer's profits is not made immediately following the liability trial. There is, instead, a further trial (a damages inquiry or account of profits) that will run to a similar timescale as the liability trial. Nonetheless, it is possible to apply for an interim payment of the damages, which will likely be awarded.

iv. Factor 4—Likelihood of Prevailing on the Merits

The cases tried in the Patents Court in England and Wales are small in number and tend to be part of a wider international dispute. Overall success rates of patent holders seeking to establish infringement of a valid patent are low.

Below is a table showing the number of first-instance judgments from 2009 to 2023, the number of judgments in which at least one patent was held valid, the number of judgments in

101. Minnesota Mining and Mfg. Co v. Johnson & Johnson, [1976] RPC 671 (England and Wales High Court–Chancery), *available at* https://academic.oup.com/rpc/article/93/25/671/1609511.

which at least one patent was held to be infringed, and the number of judgments in which at least one patent was held to be valid and infringed.[102]

Year	Total number of judgments	First-instance judgments with a finding of validity (out of the total judgments considering validity)	First-instance judgments with a finding of infringement, including conceded infringement, out of the total judgments considering infringement	First-instance judgments with a finding that a patent is valid and infringed (out of the total judgments considering both validity and infringement)
2009	24	12/23	11/15	7/14
2010	10	4/9	3/9	1/8
2011	15	5/14	5/13	1/12
2012[103]	16	10/16	6/12	4/12
2013	23	10/18	14/19	6/14
2014[104]	23	7/19	13/17	7/14
2015	12	5/11	4/6	1/6
2016	17	4/14	10/13	3/10
2017	11	3/10	6/7	2/6

102. Derived from the data published in *A User's Guide to Patents, Fifth Edition*, by Trevor Cook, WilmerHale, published by Bloomsbury Professional Law (other than 2019-21 data, which has been provided directly by Trevor Cook).

103. Excluding finding of infringement in declaration of noninfringement claim.

104. Excluding finding of infringement in declaration of noninfringement and groundless threats claims.

Year	Total number of judgments	First-instance judgments with a finding of validity (out of the total judgments considering validity)	First-instance judgments with a finding of infringement, including conceded infringement, out of the total judgments considering infringement	First-instance judgments with a finding that a patent is valid and infringed (out of the total judgments considering both validity and infringement)
2018	12	7/11	7/10	6/9
2019	16	4/15	13/13	4/12
2020	14	10/14	10/12	8/9
2021	19	7/18	13/17	4/15
2022	20	5/18	10/16	5/14
2023	17	9/16	10/16	5/15

No overall pattern can be discerned other than historically, except for 2018 and 2020, the number of judgments in which at least one patent was found valid and infringed has not exceeded 50 percent of judgments in which both issues were considered.

The consequence of these success rates is that up until recently, the court lists have been dominated by international pharmaceutical patent litigation. Generic companies have been encouraged by the rates of invalidation and the need under English law to "clear the way" in advance to avoid being enjoined upon launch (and, accordingly, bringing claims for revocation and declarations of noninfringement, targeted at those patents that were perceived to be weaker).

More recently, a large number of cases have been brought by declared standard-essential patent holders, including nonpracticing entities, in the cellular telecommunications field. In particular, declared SEP holders seek to obtain an injunction

in respect of any one UK patent in their portfolio, with a view to demanding a FRAND license to their entire global portfolio.[105] A patent holder with a large portfolio will seek to demand a high value license and will be in a position to assert a large number of patents with a view to increasing its overall chances of success.

v. Factor 5—Availability of Effective Relief

In the United Kingdom, a patent owner may launch civil proceedings for patent infringement and claim the following main types of relief:

- an injunction to stop or prevent infringement;
- delivery up or destruction of infringing goods; and
- damages or an account of infringer's profits.

Most UK patent cases settle.[106]

Interim, Final, and Springboard Injunctions. Whether to grant an injunction is up to the court's discretion and is not a remedy

105. Based on Unwired Planet Int'l Ltd. v. Huawei Technologies (U.K.) Co.; Huawei Techs. Co. v. Conversant Wireless Licensing SARL; ZTE Corp. v. Conversant Wireless Licensing SARL, [2020] UKSC 37 (UK Supreme Court) (judgment for the three appeals holding that a FRAND license can be global), *available at* https://www.supremecourt.uk/cases/uksc-2018-0214.html.

106. MICHAEL C. ELMER & C. GREGORY GRAMENOPOULOS, GLOBAL PATENT LITIGATION: HOW AND WHERE TO WIN (3d ed. 2019), Ch. 20, Table 20-2 (referring to the largest damages awards in UK patent cases as:

- Ultraframe v. Eurocell, [2006] EWHC 1344 (Pat) (England and Wales High Court–Patents), *available at* https://www.bailii.org/ew/cases/EWHC/Patents/2006/1344.html (reportedly awarding $6.15 million in damages).
- Gerber Garment Technology, Inc. v. Lectra Systems Ltd., [1997] RPC 443 (England and Wales Court of Appeals) (reportedly awarding $6 million in damages).

provided as of right. The court may grant an injunction when it considers it to be just and convenient in the circumstances, bearing in mind the need for any relief to be effective, proportionate, and dissuasive.

The following questions are considered by the judge when weighing whether to grant a preliminary interim injunction:

1. is there a serious question to be tried;
2. where does the balance of convenience lie (including a consideration of whether damages would be an adequate remedy); and
3. are there any special factors.

In practice, interim injunctions are largely limited to pharmaceutical cases involving generic pharmaceutical companies that have failed to "clear the way" before launch (e.g., by obtaining a declaration of noninfringement or revoking the patent). For a patentee to be successful, the interim injunction application must be made without delay. The patentee must give a cross-undertaking as to the damages that will be payable to the defendant in the event the injunction is eventually deemed wrongly granted because the patentee loses at trial or subsequently. Such cross-undertakings can also be in favor of third parties that suffer loss as a result of the interim injunction.

A final injunction may also be granted following a substantive trial to mandate or prevent certain acts (such as the manufacture, sale, or importation of goods held to infringe a patent). It may be stayed pending appeal, as discussed above. A final injunction might not be granted if the cost of design around is disproportionate and if the licence being demanded is excessive. Nonetheless, in the ordinary course, a final injunction will be granted following a finding of infringement.

Springboard injunctions that continue post-patent expiry may be available where the final product is not infringing but

the process by which it was developed included infringing acts. Any such injunction should reflect the advantage gained by the infringing use and not put the patentee in a better position than if there had been no infringement. These are extremely rare.

Delivery Up or Destruction of Infringing Goods. Where goods have been found to infringe patent rights, courts may order, at the request of the applicant, delivery up or destruction of any patented product in relation to which the patent is infringed or any article in which that product is inextricably comprised.

Damages or an Account of Profits. A patent owner may seek damages (relating to losses to the patent owner caused by the infringement) or an account of profits (relating to the profits made by the infringer through their infringing activities, the purpose being to quantify any unjust enrichment). Both may be claimed as alternative remedies in the pleadings. It is only after infringement has been found that the patent owner must elect damages or an account of profits.

Generally, damages are compensatory, not punitive. Where the patentee sells or manufactures products, it may claim for the lost sales of products sold by the infringer, as well as losses from sale and supply of ancillary items. Where the patentee usually licenses the patent, the measure of damages will usually be a royalty rate, based on comparable license agreements. Where the patentee neither manufactures nor sells products and does not license the patent, the court will seek to determine a notional royalty rate, applying the user principle that a royalty reflects the damage suffered. The general rule is that the damages will amount (as far as possible) to the sum of money that would put the injured party in the same position it would have been in if it had not sustained the wrong. The burden of proof in establishing the amount of damages lies with the claimant, but damages are assessed liberally.

An account of profits is rare in patent cases because, typically, a party would expect to recover more through a damages inquiry. The court will assess the overall profit and then make an apportionment.

FRAND License Determination. The UK Supreme Court[107] held in August 2020 that (a) the UK courts have the jurisdiction, and may properly exercise their power, to grant an injunction in respect of a UK patent that is an SEP, unless the implementer of the patented invention enters into a FRAND license; (b) such a FRAND license may be a global license of a multinational patent portfolio; and (c) the UK Court may determine the terms of that license without both parties' agreement.

As a consequence of this decision and the relief available to SEP owners, the English Court continues to be a leading forum for resolving global SEP-FRAND disputes.

vi. Factor 6—Cost of Litigation

Although the United Kingdom has a reputation for being a relatively expensive forum in which to litigate, costs are generally lower than in the U.S.[108]

There are a number of options available to claimants in certain circumstances that can serve to limit and control costs. This includes issuing proceedings in the Intellectual Property

---

107. *See* [2020] UKSC 37 (UK Supreme Court) (and the three appeals discussed therein), *supra* note 105.

108. Matthew Bultman, *What You Need To Know About Patent Litigation In The UK*, LAW360 (Aug. 6, 2018), https://www.law360.com/articles/1070615/what-you-need-to-know-about-patent-litigation-in-the-uk ("The 2016 Taylor Wessing report ranked the U.K. seventh in the world in cost effectiveness of enforcement, behind Germany, the Netherlands and France. It was, however, still more cost effective than the U.S., which was 26th on the report.").

Enterprise Court (IPEC) or in the High Court under the Shorter Trials Scheme.

The IPEC is a specialist IP court with a streamlined procedure, fixed costs recovery (see below), and a cap of £500,000 on the financial remedies (unless otherwise agreed by all the parties).[109] The objective of IPEC is to handle the smaller, shorter, less complex, less important, lower value actions, and the procedures applicable in the court are designed particularly for cases of that kind. It is seen, although not exclusively, as a forum for litigation by small and medium enterprises, and it has been a popular forum in which to litigate.

The Shorter Trials Scheme enables parties to benefit from resolving disputes in a shorter time period, with trials being listed more quickly and judgment being handed down within six weeks of trial.[110] It is only appropriate for the less complex cases.

vii. Factor 7—Recovery of Fees

The general principle in the UK is that the unsuccessful party is ordered to pay the costs of the successful party. Subject to limited exceptions, the court has wide discretion to make a different order after taking into account all relevant factors, including, among other things, the conduct of the parties before and during the proceedings, whether a party has succeeded on part or all of its case, the complexity of the case, as well as whether either party has refused to attempt to mediate or settle

109. *See* Intellectual Property Enterprise Court, GOV.UK, https://www.gov.uk/courts-tribunals/intellectual-property-enterprise-court (last visited Nov. 8, 2024).

110. *See* Practice Direction 57AB – Shorter and Flexible Trials Schemes, JUSTICE – GOV.UK, https://www.justice.gov.uk/courts/procedure-rules/civil/rules/practice-direction-57ab-shorter-and-flexible-trials-schemes (last visited Nov. 8, 2024).

the case. Fee shifting is usually issue-based, where a winning party's fees are discounted in relation to the issues on which it has lost. Once the court has determined whether costs are recoverable and by which party (and in respect of which issues), there is a separate process called "assessment" that determines the amount of costs recovery according to what was reasonably and proportionately incurred.

Recovery of fee determinations in the Patents Court is treated similarly to that in other UK courts, which will only award costs that are proportionate to the matters in issue. The party seeking to recover its costs must prove the reasonableness and proportionality of the amount claimed. The court can also award costs on the indemnity basis, though such an award is less common, as it is considered to be penal in nature. Where indemnity costs apply, the court will resolve any doubt that it may have as to whether the costs were reasonably incurred or were reasonable in amount in favor of the receiving party, with no requirement that the costs assessed be proportionate.

In the Intellectual Property Enterprise Court, starting October 1, 2022, the cap for costs recovery increased from £50,000 to £60,000 for the liability phase and from £25,000 to £30,000 for the damages and account-of-profits phase.[111] In addition to the overall cap, there are limits on the costs payable for each stage of the proceedings.

A patent holder that has been successful in upholding its patent should seek a certificate of contested validity from the court. The court has discretion whether to grant such a certificate, but where it is granted, then if in any subsequent

111. Part 46—Costs-Special Cases, Amount of scale costs, R. CIV. P. 46.21, JUSTICE – GOV.UK, https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part-46-costs-special-cases#amo (last visited Nov. 8, 2024); The Civil Procedure (Amendment No. 2) Rules 2022, No. 783 (L. 8), https://www.legislation.gov.uk/en/uksi/2022/783/ (last visited Dec. 11, 2024).

proceedings for infringement or for revocation of the patent in which the patentee is successful, the patentee is entitled, unless the court or the comptroller otherwise directs, to be awarded its trial costs or expenses. Such costs are generally more generous than costs assessed on a standard or indemnity basis.[112]

Parties often reach agreement as to the amount of costs to be paid by the losing party in advance of it being assessed by the court.

b. Opportunity For Defendant-Initiated Litigation

Revocation Proceedings. Under UK patent law, there are five grounds for revocation of a patent by a third party:

- Nonpatentability: that the invention is not novel or inventive, or it relates to excluded subject matter, such as business methods;
- Nonentitlement: the patent was granted to a person not entitled to it;
- Insufficiency: the patent specification does not describe the invention sufficiently to enable it to be reproduced by the skilled person;
- Added matter: the subject matter of the patent extends beyond the content of the originally filed application; and
- Unallowable post-grant extension: the projection conferred by the patent has been extended by an amendment after grant, but which should not have been allowed.

112. Patents Act 1977 c. 65 [The UK Patents Act 1977]. The approach to determining costs when the patentee has a certificate of contested validity was considered in *Optis Cellular Technology v. Apple Retail U.K. Ltd*, [2020] EWHC 3248 (Pat) (England and Wales High Court–Patents).

No standing is required to bring a claim for revocation of a patent in the UK.

Declaratory Relief. There is statutory provision in the UK Patents Act for declarations of noninfringement to be brought by any party. No standing is required.

Additionally, the English court, under its Civil Procedure Rules and its inherent jurisdiction, has a wide general power to make declarations that will serve a useful purpose, having considered justice to the claimant and the defendant, as well as whether there are any other special reasons why the court should or should not grant declaratory relief.

Over time, a range of declarations have been developed by the courts. For example, a potential infringer can seek declaratory relief in circumstances where a patent right has yet to be granted (termed *Arrow* declaratory relief after the case that first confirmed the court**'s** jurisdiction to grant such relief). An *Arrow* declaration is a declaration that the applicant**'s** own product or process, or aspects of it, were known or obvious at a particular relevant date. This arises particularly in cases where divisional patent applications are pending and pose a threat to the applicant, and where there are other factors indicating that the patentee is shielding subject matter or patents from scrutiny before the courts. The award of such a declaration provides a defense against a future claim of patent infringement. This is because if the product or process (or aspects of it) was known or obvious at the priority date of the relevant patent, then none of that patent**'s** claims can be both valid and infringed by that relevant product or process.

The English court has also confirmed that it has jurisdiction to grant declaratory relief concerning Supplementary Protection

Certificates (SPCs)[113] that have yet to be granted. Such a declaration has been sought on the basis that any application that the patentee might make seeking an SPC based on the claimant's marketing authorization would be invalid.

Another example of a declaration claim that the court will entertain is for a declaration of nonessentiality, that is to declare a particular patent is not essential to a standard.

The English court has also been willing to grant declarations of noninfringement of European patents in other jurisdictions, provided validity is not in issue.

Groundless Threats. An alleged infringer may also bring an action against the patentee for groundless threats of infringement proceedings. The "threat" is actionable if it is determined to be a "threat of infringement proceedings" following an objective two-step test. Threats need not be understood to relate only to bringing infringement proceedings in the UK, and the threat need not be directed at a particular individual for it to be an actionable threat. However, there is a "safe harbor" for patent holders to make communications for "permitted purposes" with a person who might otherwise be entitled to bring an unjustified threats action. The "permitted purposes" include notifying the recipient of the communication that the patent right exists; attempting to discover whether and by whom the patent is infringed; and giving notice that a person has a right under a patent where that person's awareness of the patent is relevant to the action that may be taken.

113. Supplementary Protection Certificates are extensions to the period of exclusivity conferred to a medicinal product covered by a patent after patent expiry. They are intended to compensate the patentee for the loss of effective protection provided by a patent due to the delay between filing a patent application and obtaining a marketing authorization.

c. Current Developments in Patent Litigation in the UK

As discussed above, the UK Supreme Court has held that the UK courts have jurisdiction to determine the terms of a FRAND license on a *global* basis in cases where a standard-essential patent holder establishes that one of its patents is valid and infringed. This has led to an influx of litigation to the UK courts, although the China Supreme Court has since confirmed that the Chinese courts also have jurisdiction to determine the terms of a global FRAND license.[114]

3. France

A key reason to start proceedings in France is the possibility of obtaining an injunction in a major EU market where both validity and infringement are adjudicated at the same time by the same court before well-regarded specialized judges. Although, as with other continental European law countries, there is no discovery or disclosure available in France, there is a well-developed practice of gathering evidence through the use of search and seizure ex parte orders. This is particularly relevant for patent holders building a multinational litigation strategy, as evidence obtained through search and seizure can usually be used in other jurisdictions. Another key reason to start litigation in France is the possibility of obtaining an advance of damages at the same time as the finding of liability (even in preliminary injunction proceedings), as well as final damages within a reasonable time frame.

114. OPPO Guangdong Mobile Communications Co. v. Sharp Co., No. 517 (China Supreme People's Court–Intellectual Property Tribunal 2020), http://gongbao.court.gov.cn/Details/f677b0f306e7dba410c62578dabead.html.

a. Global Venue Selection Factors

i. Factor 1—The Market

France is the second largest economy in the European Union and the seventh largest worldwide by GDP.[115] France's GDP is approximately $3.1 billion U.S., and around 2.2 percent of its GDP is spent in research and development.[116]

France has a large presence in a variety of sectors, such as automotive, pharmaceutical, aeronautics, chemicals, and agricultural. France has been ranked first in Europe for foreign investments and also, at a sector-based level, for foreign investment in industrial activities for the past fifteen years.[117] A number of major international companies are headquartered in France.

ii. Factor 2—The Quality of Adjudication

The quality of adjudication in France is considered high. Patent litigation is in the hands of civil professional judges (though with no technical background) for both invalidity and infringement claims. In order to increase the predictability of

115. *The 20 Countries with the largest gross domestic product (GDP) in 2024*, STATISTA (Sept. 19, 2024), https://www.statista.com/statistics/268173/countries-with-the-largest-gross-domestic-product-gdp/.

116. *Gross domestic expenditure on research and development (GERD) as a percentage of GDP in France from 2001 to 2022*, STATISTA (Oct. 25, 2024), https://www.statista.com/statistics/420952/gross-domestic-expenditure-on-research-and-development-gdp-france/.

117. *See Publication of the France Attractiveness Scoreboard, 2021 edition*, DIRECTION GÉNÉRALE DU TRÉSOR (Jan. 17, 2022), https://www.tresor.economie.gouv.fr/Articles/2022/01/17/publication-du-tableau-de-bord-de-l-attractivite-de-la-france-edition-2021. *See also New investment champion in Europe*, INVEST IN FRANCE, https://investinfrance.fr/the-new-investment-champion-in-europe/ (last visited Nov. 8, 2024).

decisions, patent litigation is within the exclusive jurisdiction of the Paris judicial first-instance court, where a specialized chamber (the third chamber, which, in turn, is subdivided into three sections consisting of three judges) is dedicated to intellectual property cases. The Paris court of appeal also includes a specialized chamber for intellectual property matters (Division No. 5, subdivided into two chambers of three judges). The highest civil court (the *Cour de cassation*) can hear patent cases through its commercial chamber.

One particularity of the French system is the possibility to seek ex parte that a search and seizure (*saisie-contrefaçon*) be carried out at the defendant's premises. This is due to the French legal system not having any discovery or disclosure-like tool to help prove infringement. As infringement needs to be evidenced by the patentee, the French system provides this search-and-seizure mechanism for the benefit of the patentee. This measure is performed in more than 80 percent of the patent infringement proceedings and conducted ahead of launching proceedings. It allows a bailiff (French public officer) to enter the premises of the defendant and to describe the accused product or process in a report, seize samples of the accused products, and take copies of any documentation evidencing not only the materiality but also the origin and the scope of the infringement (including financial documents). Once performed, the claimant has 31 days to launch patent infringement proceedings; otherwise, the seizure is automatically void and all reports, documentations, and samples must be given back to the defendant. Although such a seizure mechanism is available in all EU countries due to the EU Enforcement Directive, [118] France's extensive experience with this measure is known to be very useful for claimants, as it allows for relatively easy and

118. *See* EU Enforcement Directive, *supra* note 88.

rapid access to evidence of infringement when compared with other EU countries. And the possibility of using the seized elements in foreign proceedings is also advantageous to litigants in multiple jurisdiction litigation strategies.

Proceedings in front of civil courts are predominantly written. French judges will largely rely on the pleadings and exhibits filed by the parties. Consequently, pleadings can be quite lengthy depending on the relevant technology. An oral hearing (typically half a day per patent, or more if necessary) is set at the end of the proceedings for the judges to hear arguments from each of the parties (based on their written pleadings) and ask questions.

The use of experts, whether appointed by the parties or by the court, is extremely rare in French patent proceedings. In those cases where experts are appointed, they are required to prepare and file written reports. Although theoretically possible, in practice there is no examination or cross-examination of experts. The parties can file expert reports prepared for the purposes of foreign patent proceedings if they consider it appropriate.

Although European Patent Office decisions are not binding on French courts, French case law is generally aligned with EPO decisions. French decisions are well respected and persuasive in other foreign jurisdictions due to the aforementioned high quality of the decisions addressing both validity and infringement, as well as the size of the market in France.

iii. Factor 3—Time to Trial and Final Relief

Preliminary proceedings can be applied for ex parte or inter partes, but in practice only inter partes proceedings are used, as French procedural law provides for the possibility to have a case heard within days in case of emergency. The time frame for preliminary proceedings averages between two to four months

(and three to six months if the first-instance decision is appealed). This time frame can be shortened to within weeks or even days in case of urgency (which is not a condition to launch preliminary injunction proceedings).

First-instance patent infringement proceedings "on the merits" (main action as opposed to preliminary proceeding) where a counterclaim for invalidity is raised usually last between 18 months to two years. In cases where only infringement or invalidity is raised, the time frame is 12 to 18 months. In appeals to the Paris court of appeal, a decision is usually handed down in two years. Importantly, the appeal is heard *de novo*. Proceedings brought before the highest civil court usually last around 18 months but can only concern points of law.

Decisions are immediately enforceable, even if an appeal is lodged.

Although damages can be sought within the liability proceedings, it is more common for the claimant to seek an advance on damages and to start a second phase of the proceedings once there is a finding of infringement from the first-instance judges. In such cases, an advance on damages is awarded to the patentee, and the defendants are forced to render account on the scope of the infringement. This second phase lasts less than a year.

iv. Factor 4—Likelihood of Prevailing on the Merits

The Paris courts are a jurisdiction where patents are invalidated in about a third of cases, held valid but not infringed

in about another third of cases, and held valid and infringed in a third of cases.[119]

v. Factor 5—Availability of Effective Relief

Injunctive Relief. In France, the grant of an injunction is "as of right" once the court confirms infringement (and the patent is upheld if validity is contested), even if an appeal is lodged. The injunction applies to any act of infringement, i.e., manufacturing, importing, offering for sale, selling the product at stake, or implementing the patented process.

Preliminary Injunctions. Preliminary injunction proceedings consider both validity and infringement of the patent-in-suit, including the merits, but on a very short time frame. The proportionality principle may lead judges to refrain from granting a preliminary injunction, but it has been seldom applied. To obtain a preliminary injunction, validity and infringement should not be seriously challengeable. An advance on damages can also be requested along with the preliminary injunction order. Until recently, the threshold to obtain a preliminary injunction was considered quite high in France because of the need for a thorough assessment of the validity and infringement of the patent-in-suit, and such orders had been hard to obtain (see further below).

Availability of Substantive Damages. Over the past twenty years, French legislators have amended the law in order to increase the damages that can be claimed by patent owners (and licensees) to better reflect the damage suffered.

Recovering damages is therefore part of the patent infringement proceedings, whether it be on the merits (the main

119. ELMER & GRAMENOPOULOS, *supra* note 1066, *Chapter 22: France* (stating that the average patentee win rates for French designation of European patents from 2006-16 was 39 percent).

action) or in preliminary proceedings. As mentioned above, a patentee can claim an advance on damages within preliminary injunction proceedings[120] or within proceedings on the merits. In the latter case, the damages are finally assessed in a second phase of the proceedings (after the liability judgment has been handed down). In a recent case, the Paris court awarded the highest ever amount of advance on damages for a patent case (€28 million, around $34 million U.S.).[121]

Following a judgment holding infringement and awarding an advance on damages, it is fairly common for parties to reach a settlement before the court concludes its damages assessment.

vi. Factor 6—Cost of Litigation

France is generally seen as a reasonable venue for the costs of litigation when compared to common law systems. As there are no court fees in France, the costs are limited to attorneys' fees. At first instance, in cases where both validity and infringement are at stake, the costs usually range between €150,000 and €500,000, depending on the complexity of the case. Costs may be higher for high-stakes cases.

120. *See* Eli Lilly vs Zentiva, RG 19/06927 [Paris Court of First Instance] Jan. 7, 2021 (awarding an advance on damages of EUR 4 million (i.e., approximately USD 4.9 million) along with a preliminary injunction), *rev'd on appeal*, but only in relation to the advance on damages, in Zentiva vs Eli Lilly, RG 21/01880 [Paris Court of Appeal] Nov. 9, 2021; *see also* Novartis vs Teva Santé, RG 16/15196 [Paris Court of First Instance] June 7, 2018 (granting almost EUR 14 million (approximately $17 million U.S.) along with a preliminary injunction).

121. *See* Eli Lilly vs Fresenius Kabi, RG 17/10421 [Paris Court of First Instance] Sept. 11, 2020.

vii. Factor 7—Recovery of Fees

In France, the winning party can claim reimbursement of its attorneys' fees. But the grant of attorney fees and the amount awarded are within the exclusive discretion of the court. There are therefore no specific rules for the determination of the amount to be awarded. Usually, the award can range between 20 to 70 percent of the attorneys' fees.

b. Opportunity For Defendant-Initiated Litigation

Defendants in France can initiate invalidity actions against a patentee where they show that they have an interest in invalidating a particular patent. The grounds for revoking a patent are lack of novelty, inventive step, or industrial application; insufficiency of disclosure; added matter; or undue extension after limitation or opposition proceedings.[122]

Defendants can also bring an action seeking a declaration of noninfringement. This action is divided into two phases. In the first amicable phase, the defendant must invite the patentee to give its opinion as to whether the relevant product or process (the details of which have been provided by the defendant) constitutes an infringement. If the patentee concludes that there is infringement or in case of lack of reply, the defendant can then launch the second phase, the judicial phase, by serving a summons for declaration of noninfringement upon the patentee.

In FRAND-specific cases, defendants have brought cases in France based on alleged contractual breach of the patentee's obligation to grant a FRAND license in accordance with its declaration made to the European Telecommunications

122. French Intellectual Property Code, Article L. 613-25 IPC and Article L.614-12 IPC, which refers to Article 138 § 1 of the European Patent Convention (French designation of European patents).

Standards Institute, the recognized European standards body dealing with telecommunications, broadcasting, and other electronic communications networks and services. French courts have recognized jurisdiction to hear these claims.[123]

c. Current Developments in Patent Litigation in France

One notable development in French patent litigation is that France has entered into the worldwide fray of anti-anti-suit injunctions in FRAND cases. As anti-suit injunctions are not legally admissible within European courts, anti-suit injunctions had been seldom addressed and only within the context of conflict between non-European state court and an arbitral tribunal, and not concerning patents. But in *IPCom v. Lenovo*, a case concerning standard-essential patents, the French court ordered an anti-anti-suit injunction and considered that this measure was admissible, as the anti-suit injunction had been granted by a non-European court and was grounded on the merits to protect the right of the patentee to litigate its French patents in France.[124]

Another recent development is the increasing rate of success of preliminary injunction proceedings. Traditionally, preliminary injunction proceedings were difficult to obtain, as

123. TCL v. Philips, ETSI, RG 19/02085 [Paris Court of First Instance] Feb. 6, 2020; Xiaomi v. Philips, ETSI, RG 20/12558 [Paris Court of First Instance] Dec. 7, 2021, Order.

124. IPCom v. Lenovo, RG 19/59311 [Paris Court of First Instance] Nov. 8, 2019; IPCom v. Lenovo, Motorola, RG 19/21426 [Paris Court of Appeal] Mar. 3, 2020 (affirming first instance court decision). It is not possible to grant anti-anti-suit injunctions within courts of the European Union due to the Brussels Regulation, which does not authorize the jurisdiction of a court of a Member State to be reviewed by a court in another Member State.

doubts on either validity or infringement would lead to a dismissal of the claim. The threshold seems to be lower than before, as only serious doubts can lead to a dismissal of the case. In practice, patents that have survived opposition proceedings or that have been successfully litigated in another European country have more chances to pass that threshold, as evidenced by the increase in preliminary injunctions handed down by French judges.

Another recent development in French case law is the confirmation by the Higher Civil court (*Cour de cassation*)[125] of the possibility to obtain cross-border injunctions on the basis of European Regulations but also on the basis of French international private law.

4. The Netherlands

The District Court of The Hague and the Court of Appeal of The Hague are sophisticated patent forums with judges that often have technical backgrounds. Traditionally, Dutch courts are known for their willingness to grant cross-border injunctions and efficient proceedings. Also, although no disclosure system applies, Dutch law offers the possibility of relatively efficiently obtaining evidence through seizure of documents. Patent litigation based on standard-essential patents in the Netherlands is common in view of the Courts' stance toward alleged negotiation-delaying tactics. Decisions from the Court of Appeal of The Hague require implementors to partake in technical discussions and constructively cooperate in negotiations toward a license agreement in order to avoid a finding of unwillingness.

125. Cass. 1st civil Ch., 29 June 2022, RG 21-11.085, Hutchinson v. Tyron Runflat et al.

a. Global Venue Selection Factors

i. Factor 1—The Market

The Netherlands is home to the headquarters of several top-500 publicly traded companies. Additionally, many large foreign companies have subsidiaries in the Netherlands or use the Netherlands as their distribution hub and point of entry to Europe. This is significant because—as a rule—the presence of a Dutch subsidiary is sufficient for the Dutch court to assume jurisdiction over its foreign parent companies. Relief is available against the Dutch subsidiaries as well as their foreign parent companies. The relief is not necessarily restricted to the Netherlands; if the Dutch subsidiary acts across the Dutch borders, cross-border relief is available, and to the same extent against any co-sued foreign parent companies. This makes the Netherlands an attractive jurisdiction for international patent litigation.

The Netherlands is geographically small but densely populated, and its economy is considerable. In 2023, GDP was at $62,536 U.S. per capita for a total of $1.12 trillion U.S.[126] About 2.3 percent of GDP is spent on research and development.[127]

ii. Factor 2—The Quality of Adjudication

Patent litigation in the Netherlands is concentrated before the specialized first-instance and appeal courts of The Hague. As a result, patent cases are dealt with by experienced judges with good technical understanding and who handle a significant number of patent cases each year. This generally leads to excellent quality and predictable adjudication.

126. *Netherlands*, THE WORLD BANK, https://data.worldbank.org/country/NL (last visited Nov. 8, 2024).

127. *Gross domestic spending on R&D*, OECD DATA, https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm, (last visited Nov. 8, 2024).

The judiciary is fully independent, with judges that are appointed for life. The Netherlands consistently ranks in the top 10 of least corrupt countries in the world.[128] The Netherlands patent system is not generally thought of as biased against plaintiffs who do not manufacture or sell the patented products in the Netherlands (nonpracticing entities) or biased in favor of domestic over foreign litigants.

Dutch procedural law, including its implementation of the EU Enforcement Directive,[129] provides litigants with several options to retrieve evidence that is in the domain of the opposing party (or an unrelated third party). Moreover, the amount of evidence required to succeed depends on the level of substantiation the defendant puts forward when contesting. As a result, if a plaintiff can make it sufficiently plausible that there likely is infringement, it will usually be able to gather the required evidence to prove its case.

Dutch courts apply established European Patent Office case law on validity, most importantly the so-called "problem-solution approach" for assessing inventive step.[130] Dutch courts will consider the outcome of EPO opposition proceedings (in particular Technical Board of Appeal decisions) as well as any decisions of experienced foreign colleagues and will treat them as persuasive (but nonbinding) viewpoints. They will nevertheless independently assess the merits of all issues based on the evidence before them.

---

128. *See Corruption Perceptions Index*, TRANSPARENCY INT'L, https://www.transparency.org/en/cpi/2019/ (last visited Nov. 8, 2024).

129. *See* EU Enforcement Directive, *supra* note 88.

130. In the problem-solution approach, (i) the "closest prior art" is determined, followed by (ii) establishing the "objective technical problem" to be solved by the distinguishing features, and (iii) considering whether the claimed invention, starting from the closest prior art and the objective technical problem, would have been obvious to the skilled person.

Decisions by the courts of The Hague are often considered representative of the "continental" European approach. Over the last ten years, the UK Supreme Court has at least twice explicitly relied on Dutch court opinions (on inventive step in *Conor v. Angiotech*[131] and on equivalence in *Eli Lilly v. Actavis*[132]) when reviewing Court of Appeal decisions.

Dutch courts decide cases based on the legal briefs submitted by the parties, the exhibits filed, and the arguments made by the advocates during the one and final court hearing, which usually lasts no longer than a day. Cases are normally decided without live examination or cross-examination of experts or witnesses, but meaningful expert involvement is possible through written expert declarations and informal questioning by the court. Technical experts need not be local—the courts are used to handling written and oral testimony in English, and foreign experts are regularly relied upon.

Dutch civil procedure does not provide for an obligation to surrender all relevant evidence (i.e., there is no discovery or disclosure). Evidence that is known to exist (such as documents or samples) can, however, be seized and secured through an ex parte evidence seizure. The evidence must be located in—or, e.g., regarding electronic files, accessible from—the Netherlands, and the standard of proving infringement is low. Similar to the French concept of the *saisie-contrefaçon*, a claimant may obtain leave to have a bailiff (a Dutch public officer) enter the premises of the defendant, describe the accused product or process in a report, and seize samples of the accused products or other pieces of evidence. Evidentiary seizures can also be

131. Conor Medsystems Inc. v. Angiotech Pharms. Inc., [2008] UKHL 49 (UK House of Lords), *available at* https://publications.parliament.uk/pa/ld200708/ldjudgmt/jd080709/conor-1.htm.

132. Actavis v. Eli Lilly, [2017] UKSC 48 (UK Supreme Court), *available at* http://www.bailii.org/uk/cases/UKSC/2017/48.html.

used to assist litigants in other jurisdictions. Evidentiary seizure is of a preservatory nature only. Subsequent access to seized evidence can be obtained through inter partes access proceedings, which are possible in preliminary injunction and merits proceedings. After performance of the seizure, the claimant must launch patent infringement proceedings within a set term; otherwise, the seizure is automatically void and all reports, documentation, and samples must be returned to the defendant.

iii. Factor 3—Time to Trial and Final Relief

Permanent relief can be acquired by litigating patent cases under an accelerated regime, which features a predetermined procedural timetable. These proceedings result in a first-instance merits decision in a time frame of 12-18 months.

Dutch law also allows for inter partes preliminary relief at very short notice: normally a hearing in up to eight to 16 weeks and a decision two to four weeks later. In extremely urgent situations, these timelines can be even shorter.

The courts handle validity and infringement within the same proceedings, both in preliminary and merits proceedings. The mere pendency of parallel invalidity or opposition proceedings as such is therefore not sufficient for a stay. In general, it is rather difficult for a patentee to successfully apply for deviation from the procedural timetable. Exceptions do occur, however; e.g., if there already is a first-instance decision on the merits invalidating the patent, or if a final decision from the Technical Boards of Appeal is forthcoming very close to the projected conclusion date of the Dutch proceedings.

As a rule, injunctive relief decisions in patent cases—both preliminary and permanent—are enforceable notwithstanding appeal, and enforcement of a judgment pending appeal usually does not require placement of a bond. The enforcement of a

decision that is later overturned results in liability for the resulting damages for the enforcer.

Dutch courts have a discretionary power to bifurcate assessment of damages, and litigants usually request such bifurcation. In practice, damage cases rarely go to trial. Due to the powerful, immediately enforceable first-instance injunctions, settlement of patent cases is much more common. Plaintiffs that insist on a court-determined damages award can initiate the damages proceedings notwithstanding appeal against the first-instance infringement decision. The damages award itself, as a rule, is also enforceable notwithstanding appeal.

First-instance decisions, both preliminary and permanent, are open to appeal at the specialized Court of Appeal of The Hague. Appeal proceedings consist of a *de novo* hearing of the case (facts and law) by three judges. They take between 12 and 18 months, but the timeline can be greatly accelerated—three to six months or shorter, if necessary—particularly in preliminary injunction proceedings. Appeal decisions may be further appealed before the Supreme Court, where proceedings may take between 1.5 and two years. No leave is required. Supreme Court appeal is limited to a review on error of law.

iv. Factor 4—Likelihood of Prevailing on the Merits

Because of the absence of bifurcation, a patentee must succeed both on validity and infringement to prevail. During the period of 2016-2021, patentees were successful in obtaining a finding of infringement in around 35 percent of judgments. The odds of succeeding were higher in preliminary injunction proceedings (around 42 percent) than in merits proceedings (around 30 percent). The appeals court is generally seen as somewhat more patentee-friendly than the first instance court.

In the same period, 30 percent of the appeal decisions overturned a first-instance decision, often in favor of the patentee.[133]

v. Factor 5—Availability of Effective Relief

Preliminary Relief. Preliminary relief is generally available in the Netherlands through inter partes preliminary proceedings. Preliminary relief proceedings are essentially a mini-trial on the merits at very short notice: normally a hearing in eight to 16 weeks and a decision two to four weeks later. In extremely urgent situations, these timelines can be even shorter. The court will form a preliminary opinion on validity and infringement. In addition, the law requires the existence of an urgent interest in an injunction. This urgency requirement, however, is not very strict. Dutch Supreme Court case law assumes that urgency exists as long as there is a continuing infringement or the threat thereof. In recent lower court case law, it is considered that maintaining an urgent interest requires swift action. An urgent interest may be lost, therefore, if six to 12 months have gone by without a proper justification. An injunction may furthermore be denied if a balancing of interests requires so. The judge in preliminary injunction proceedings must give consideration, inter alia, to the provisional nature of the judgment and the far-reaching consequences of a possible injunction for the defendant, on the one hand, and to any damages suffered by the claimant if an injunction were not granted, on the other hand. FRAND disputes are in principle deemed unsuitable for preliminary injunction proceedings.

In addition to inter partes preliminary relief, ex parte relief may be obtained in highly exceptional cases, if the patentee can

133. These figures are compiled on the basis of yearly case law updates by Gertjan Kuipers at the Dutch Patent Conference. The editors of this *Framework* were unable to obtain more recent figures.

show (a) a prima facie valid title, (b) the prima facie threat of infringement, and (c) irreparable harm if the patentee would have to await the outcome of inter partes preliminary proceedings. As mentioned above, a protective letter can be filed to try to avoid or limit the scope of ex parte measures.

Injunctive Relief. As a rule, injunctive relief is available to a patentee whose patent is held to be valid and infringed. Breach of an injunction results in severe civil penalties, which are due immediately and payable to the plaintiff.

Exceptions where injunctive relief can be avoided despite a finding of infringement include situations wherein granting injunctive relief is (a) disproportional in view of the fundamental rights involved; (b) contrary to the patentee's contractual or legal obligations (e.g., in standard-essential patent disputes); (c) contrary to a compelling societal interest; or (d) an abuse of rights. Such defenses are rarely successful.

Other Relief. Other available relief includes recall and destruction of infringing products, public notification of the decision, the obligation to disclose details regarding suppliers and customers, and the obligation to disclose details regarding numbers and profits.

Availability of Substantial Damages. Dutch proceedings are based on a system of compensatory damages. Damages awards do not have a punitive element. The assessment can be based on lost profits of the patentee or on surrender of realized profits by the infringer. Damages can also be estimated, e.g., based on a fictitious royalty.

Cross-border Relief. In both preliminary and permanent injunction proceedings, cross-border relief covering the whole territory protected by a European patent is available in cases where Dutch defendants who act across Dutch borders are involved. Cross-border relief is also available against foreign defendants involved in the same cross-border activities, e.g.,

parent companies of Dutch defendants. There are examples wherein the mere presence of a Dutch European distributor of an infringing product was sufficient for granting cross-border relief against the product's foreign manufacturer and customers as well. If the defendant raises an invalidity defense, *permanent* cross-border relief is unavailable or will be stayed,[134] but an invalidity defense does not interfere with availability of a *preliminary* cross-border injunction.[135]

Preliminary Civil Seizure of Infringing Products. Dutch law provides for the possibility to preliminarily seize or attach products that allegedly infringe IP rights. The procedure is ex parte, fast, relatively easy, and cost-effective. A seizure or attachment request must be filed with the competent court, mentioning the IP rights invoked and the reasons infringement is suspected. The request will generally be allowed by court decree within a couple of days. On the basis of this decree, a bailiff (if necessary, with the assistance of the police) can enter the premises of the alleged infringer and make a detailed description of the stock (numbers and product codes) or physically seize the stock and store it elsewhere. Preliminary seizure or attachment is a "conservatory" measure: the effect is that the owner of the seized or attached products is no longer entitled to trade the products pending the infringement proceedings on the merits, which must be initiated after execution of the seizure.

---

134. Roche Diagnostic Corp./Primus II, ECLI:NL:HR:2007:BA9608 (Netherlands Supreme Court Nov. 30, 2007). On the basis of Art. 24(4) of Regulation (EU) No 1215/2012 ("Brussels I bis"), the Courts of the Member State where the (foreign) patent is registered have exclusive jurisdiction regarding matters of validity of the patent.

135. Solvay SA v. Honeywell Fluorine Prods. Europe BV, C-616/10 (CJEU 2012), *available at* https://curia.europa.eu/juris/liste.jsf?num=C-616/10&language=EN.

Border Detention Measures. The Dutch customs authorities have become rather sophisticated (upon the request of IP proprietors) in detecting and detaining infringing products entering the European market via the Netherlands. IP proprietors can request the cooperation of customs by filing a border detention request, listing the relevant IP rights, and providing sufficient details for recognizing the goods upon arrival. When customs authorities encounter products that conform to a border detention request, they will normally retain the products and inform the IP proprietor forthwith, who can then follow up with appropriate action (e.g., inspect and, if appropriate, initiate civil proceedings).

vi. Factor 6—Cost of Litigation

Dutch litigation is relatively cost-effective, in part due to the absence of discovery or disclosure. Nevertheless, the costs of litigation vary significantly with the complexity of the case and the amount of expert involvement required. Although the contributors to this publication have not located any published data on this subject, the observation of those who actively practice Dutch patent litigation is that straightforward patent cases can be tried for under €100,000 in first instance, whereas a case on a highly complex patent can cost up to around €500,000. As a rough rule of thumb, a full appeal on facts and law will cost about 75 percent of the first instance. Nonpatent defenses (e.g., FRAND defenses that require extensive third-party input) can add significantly to these numbers.

vii. Factor 7—Recovery of Fees

The winning party in Dutch patent litigation is entitled to be compensated by the losing party for its "reasonable and proportionate" legal costs. To provide a yardstick for what are reasonable and proportionate legal costs, a cap is set by the court depending on the complexity of the case that ranges from

€10,000 for a simple case in preliminary injunction proceedings to €250,000 in highly complex merits proceedings.[136] These caps include the fees of legal and patent counsel but exclude disbursements such as expert costs. The parties may independently negotiate a cost amount to avoid a hearing. The order to pay legal costs will routinely be enforceable notwithstanding appeal.

b. Opportunity For Defendant-Initiated Litigation

Invalidity Actions. Dutch invalidity actions are open to anyone and can be instigated at any point during the lifetime of a patent. They are reasonably fast and are therefore suitable to influence other jurisdictions, in particular jurisdictions that have bifurcated validity and infringement assessments.

Declaratory Actions. Dutch civil law contains a broad provision allowing a party to apply for any declaratory judgment regarding a legal relationship, provided that it can show a legal interest in obtaining such declaratory judgment. Examples of declaratory relief in patent cases that the Dutch court has ruled upon include declarations of noninfringement, declarations of obviousness of a product over the state of the art on a particular date (i.e., "*Arrow* declarations"),[137] [138] and declarations of "FRAND-ness" of license offers in a standard-

136. *Indicatietarieven in Octrooizaken Rechtbank Den Haag* (Sept. 1, 2020), *available at* https://www.rechtspraak.nl/SiteCollectionDocuments/indicatietarieven-in-octrooizaken-rb-den-haag-1-september-2020.pdf.

137. For description of "*Arrow* declarations," *see supra* note 11 and underlying commentary text.

138. *E.g.*, MSD v. Generics, *IEPT20080213* (District Court The Hague Feb. 13, 2008), *summary available at* https://www.boek9.nl/items/iept20080213-rb''-den-haag-msd-v-generieken.

essential patent dispute.[139] Although not yet tried in practice, it is likely that the provision also allows a defendant to apply for the determination of appropriate license terms in such disputes, and in other cases where a patentee is contractually or legally obliged to provide a license.

Preliminary injunction proceedings result in a reasoned judgment on both validity and infringement in a matter of weeks. These proceedings are therefore useful to gain fast, meaningful relief that is suitable for use in a counterattack. Pure invalidity actions in preliminary injunction proceedings, however, are generally thought to be impossible.

c. Current Developments in Patent Litigation in the Netherlands

Due to the case load at the District Court of The Hague, first-instance proceedings (whether according to the "accelerated regime" or in regular merits proceedings) currently may take longer than usual to result in a judgment. Whereas accelerated patent infringement cases in the past resulted in a decision in 12 to 15 months, it may now take 18 months to two years before a judgment is rendered. There are voices calling for the creation of a second specialized IP court in the Netherlands, but no plans to that effect have been made yet.

The District Court of The Hague has recently indicated that it deems both preliminary injunction proceedings and merits proceedings in accordance with the "accelerated regime" unsuitable for FRAND disputes. Therefore, owners of standard-essential patents are left to regular merits proceedings, which

139. Archos v. Philips, ECLI:NL:RBDHA:2017:1025 (District Court The Hague Feb. 8, 2017), *available at* https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2017:1025.

are generally on a slower pace but provide more possibilities for tailored procedural arrangements.

The District Court of The Hague nevertheless continues to be an attractive venue for cross-border actions. In two recent cases, the District Court of The Hague accepted cross-border jurisdiction. One of these cases is a "standalone" FRAND case, and the other concerns a request for an anti-anti-suit injunction (which was not granted in part due to a lack of urgent interest).[140]

C. Asia

1. China

In recent years, plaintiffs have found success in all three Chinese Intellectual Property Courts. For example, foreign parties have had an average win rate reaching over 68 percent before the Beijing Intellectual Property Court.[141] In addition, China issued the Fourth Amendment to China's Patent Law, effective mid-2021, which signifies its overall direction in making China a more competitive forum for patent enforcement, with increased damage awards and provisional relief measures and conferring more power on administrative intellectual property enforcement. Thus, it is expected that this venue will continue to be attractive for both domestic and foreign plaintiffs who want to take advantage of the low

140. *See* Vestel v. Phillips et al;, ECLI:NL:RBDHA:2021:14372 (District Court The Hague Dec. 15, 2021), *available at* https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2021:14372; Ericsson v. Apple, ECLI:NL:RBDHA:2021:13881 (District Court The Hague Dec. 16, 2021), *available at* https://linkeddata.overheid.nl/front/portal/document-viewer?ext-id=ECLI:NL:RBDHA:2021:13881.

141. *Beijing Intellectual Property Court: The winning rate of foreign parties in foreign-related civil cases is nearly 70%* (Oct. 18, 2019).

litigation costs, fast first-instance proceedings on the merits, and available remedies.

a. Global Venue Selection Factors

i. Factor 1—The Market

Asia, particularly China, has long been an important manufacturing region and sales market for multinational firms. According to statistics released by the National Bureau of Statistics of China in August 2023, the national economy continued to recover, production and demand were basically stable, and employment and prices generally held steady.[142] In particular, in July 2023, the total value added of industrial enterprises grew by 3.7 percent year on year, wherein the value added of mining increased by 1.3 percent, manufacturing went up by 3.9 percent, and the production and supply of electricity, thermal power, gas, and water grew by 4.1 percent.[143]

Increasing economic activity and expansion of market size has resulted in a significant increase in the number of patent filings in China. In June 2023, the World Intellectual Property Organization announced that Chinese applicants filed 70,015 patent applications through the Patent Cooperation Treaty system in 2022, ranking first ahead of other countries such as the U.S. (59,056 applications) and Japan (50,345 applications).[144] This reflects China's efforts to transform from a major

142. *See* Press Release, National Bureau of Statistics of China, National Economy Sustained the Steady Recovery in July (Aug. 15, 2023), http://www.stats.gov.cn/english/PressRelease/202308/t20230815_1941964.html.

143. *Id*.

144. *See* PCT YEARLY REVIEW 2023, WORLD INTELLECTUAL PROP. ORG. (2023), https://www.wipo.int/edocs/pubdocs/en/wipo-pub-901-2023-en-patent-cooperation-treaty-yearly-review-2023.pdf.

intellectual property rights importer into a major intellectual property rights creator.

ii. Factor 2—The Quality of Adjudication

Specialized Intellectual Property Courts. Since November 2014, China has established four specialized intellectual property courts (or tribunals) in Beijing, Shanghai, Guangzhou, and Hainan Free Trade Port. Notably, a nationwide unified appeal court has been established in Beijing to exclusively hear appeals for all invention and utility model patent-related cases. As more patent litigation cases are lodged in China, the Chinese courts are establishing a substantial track record with patent litigation. This can minimize the uncertainties for both sides, especially in cases involving some specific issues or subject matter such as standard-essential patents or biotechnology. Furthermore, judges in specialized intellectual property courts or tribunals generally have extensive experience in IP and are normally assisted by technical advisors in cases that require technical knowledge, including patent infringement cases.

Smart Court. In recent years, China has also strived to build a "smart court" system to modernize its trial and court system, facilitate court management, and automate and digitalize the adjudication process. The scope of digitalization includes online case filing, online payment, online video hearings, and evidence storage and processing using blockchain. According to the Supreme People's Court, 10.7 million cases were filed online in 2022 via the "People's Court Online Service" mobile terminal, an average of 61 cases every minute; and 92.64 million cases were served online, with a year-on-year increase of 123 percent.[145] To regulate online litigation, the Supreme People's

145. *See SPC: In 2022, the people's courts filed more than 10 million cases online* (Feb. 15, 2023).

Court has enacted a comprehensive set of rules and procedures—the Rules of Online Litigation of People's Court (effective August 1, 2021)—requiring online litigation to be "impartial and efficient, legal and optional, right-protection oriented, convenient for the people, and safe and reliable."[146]

Choice of Jurisdiction. Litigants in China are allowed to choose the jurisdiction (or specifically a province or a city) to commence proceedings based on the place where the allegedly infringing acts take place, i.e., where the infringing products were made, used, offered to sell, sold, or imported. In practice, litigants tend to commence proceedings in a familiar jurisdiction or a jurisdiction that is favorable to the litigant, such as the place where the litigant conducts business, the place with generally higher chance of success for patent litigation, or—for cases involving a foreign patent owner—the place that has a reputation of being fair to foreign litigants. For strategic purposes, a litigant may try to establish a link between its targeted jurisdictions with the infringement, such as by purchasing the infringing product from a seller or distributor based in the targeted jurisdictions.

No Discovery. As there is no extensive documentary discovery in China and no formal seizure or inspection procedure as is common in many European jurisdictions, litigants often have to engage investigation firms to assist in procuring sufficient evidence in support of their case. During the evidence gathering process, when certain important evidence is procured, it is common to conduct evidence preservation. If certain evidence proving infringement or damages is not available or accessible to the plaintiff, the plaintiff can request an order from the court to preserve the

146. *See The SPC Releases the Rules of Online Litigation of People's Court*, [CHINA] DALIAN MARITIME COURT (Sept. 27, 2021), https://www.dlhsfy.gov.cn/en/index.php?m=content&c=index&a=show&catid=107&id=1247.

evidence, i.e., ordering the defendant or third parties having possession of the evidence to produce the evidence to the court. Typically, such evidence will include financial books showing damages and samples of accused products showing infringement.

iii. Factor 3—Time to Trial and Final Relief

Patent litigants in China generally can secure relief within a reasonable (and reasonably predictable) time frame. Compared to the U.S., where time to trial in patent cases can take up to three to four years, patent litigation in China tends to have a shorter time frame because adjudication normally takes place in specialized intellectual property courts, and there are no discovery proceedings.

The time required to complete patent invalidation proceedings in China is generally six months but may be reduced to five (for an invention or utility model patent) or four (for a design patent). The time to complete a patent infringement proceeding through appeal can take up to two or more years, with the first-instance proceeding taking approximately nine to 18 months and the second-instance proceeding taking approximately six to nine months (or longer on a case-by-case basis).

Further, court proceedings in China typically are not stayed pending the completion of an invalidation proceedings before the Patent Reexamination Department of the China National Intellectual Property Administration (CNIPA), although damages awards and permanent injunctions are generally stayed pending the outcome of an appeal.

iv. Factor 4—Likelihood of Prevailing on the Merits

With the specialized intellectual property courts and reform measures and mechanisms introduced by these specialized courts, China provides patent litigants, including foreign litigants, a reasonable chance of prevailing on the merits of the case.

In China, methods for diagnosis or treatment of diseases are not patentable, while software is patentable. All patentable technologies are generally equally enforceable in China, including pharmaceutical patents.

v. Factor 5—Availability of Effective Relief

A wide range of relief is available in China, including preliminary injunctions, damages awards, and permanent injunctions. Each type of relief provides different benefits to litigants.

Preliminary Injunction. An injunction may be sought by a patent holder to put a defendant out of the infringing business, increase the patent owner's market share, or serve as a strong settlement lever in the patent holder's favor. To obtain a preliminary injunction in China, litigants must satisfy the following factors: (1) whether the claimant's request has a factual ground and a legal basis; (2) whether failure to take preservation measures will cause irreparable harm to the legitimate rights and interests of the claimant, or cause difficulty in the enforcement of the ruling for the case; (3) whether the harm that would have been caused by the failure to take preservation measures exceeds the damage that would have been caused to the defendant by conduct preservation measures; (4) whether an injunction would prejudice the public

interest; and (5) any other factors that need to be considered.[147] If granted, a preliminary injunction takes immediate effect. Nevertheless, obtaining a preliminary injunction in patent infringement cases has historically been difficult given the concern that the patents might ultimately be held at trial to be noninfringed or invalid on merits; the Supreme People's Court has issued opinions and guidance warning against granting preliminary injunctions for this reason.[148] On the other hand, courts are more inclined to grant preliminary injunctions in design patent infringement cases where it is relatively easy to determine infringement.[149]

Monetary Damages. The award of damages accounts for an overwhelming majority of the remedies for patent infringement cases and is determined by the factors stipulated under Article 71 of the Patent Law of the People's Republic of China: (i) the patentee's actual losses caused by infringement; (ii) the infringer's profits from the infringement; (iii) a reasonably multiplied amount of the royalties from the patent; or (iv) statutory-type damages within the range of RMB 30,000 to RMB

147. *See* Provisions of the Supreme People's Court on Several Issues Concerning Application of Law in Review of Cases Involving Behavior Preservation in Intellectual Property Right Disputes, the Supreme People's Court (Aug. 27, 2019), https://splcgk.court.gov.cn/gzfwww/sfjs/details?id=ff8080816c22fc85016cd0bf71dd0d99.

148. *See* Zhou Xi et al., *China IP Law Alert: The Supreme People's Court seeks public comment on its proposed enhanced sanctions for IP infringement*, BAKER MCKENZIE (June 29, 2020), https://www.lexology.com/library/detail.aspx?g=243d9400-deab-48ee-9b73-d55da4895ee4.

149. *See* Guanyang Yao & Xiao Wang, *Understanding Design Patent Protection*, WORLD TRADEMARK REVIEW (Sept. 30, 2021), https://www.worldtrademarkreview.com/regionindustry-guide/china-managing-the-ip-lifecycle/2022/article/understanding-design-patent-protection.

5 million (approximately $4,700 to $782,000 U.S.).[150] In fact, the current Patent Law has substantially increased the amount of statutory damages available to the patentee and has made available punitive damages of up to five times the amount of damages determined against willful infringement, indicating that China is determined to strengthen the availability of damages to patentees.[151] According to the 2020 China Patent Investigation Report issued by the CNIPA—which investigated 24 provinces (autonomous regions, municipalities), 15,000 patentees, and 42,000 patents during the five-year period from 2016 to 2020—7.3 percent of patent infringement court cases ended up with over RMB 1 million in damages, whether from court order, mediation, or settlement, which is 4.4 percent higher than that during the preceding five years.[152]

Permanent Injunction. When a court finds infringement, it usually issues a permanent injunction as part of the remedies award to order the defendant to cease the infringing acts so long as the patent is valid and the infringing acts are continuing. However, there are cases where the court has found infringement but refused to grant any permanent injunction due to public interest concerns. For instance, in 2008, the Supreme People's Court awarded an ongoing royalty but not a permanent injunction against a defendant that operated a power plant using an infringing desulfurization process, in part because the power plant's closure would have a detrimental

150. *See* Defeng Song, *Understanding the Fourth Amendment of Chinese Patent Law*, FIELDFISHER (July 27, 2021), https://www.fieldfisher.com/en/locations/china/insights/understanding-the-fourth-amendment-of-chinese-patent-law.

151. *Id.*

152. *See Report: Over 30% Current Patents Commercialized in China*, CHINA SERVICES INFO (updated June 8, 2021).

impact on the local residents.[153] Any permanent injunction granted by the court of first instance is stayed pending appeal. Such limitation is not applicable to a preliminary injunction, as a preliminary injunction is of interlocutory nature and takes effect throughout the entire proceedings.

Customs Seizure. An order of customs seizure allows customs authorities to seize and eventually destroy infringing goods, which, along with the threat of court litigation, may put additional pressure on the accused party.

vi. Factor 6—Cost of Litigation

The cost of litigation in China varies from case to case. Attorney fees and court fees are commonly incurred in litigation proceedings in China, but there are also other prelitigation costs specific for Chinese proceedings.

For costs borne during the evidence gathering process as described in Factor 2—Quality of Adjudication, the litigant could seek to recover all these costs from the defendant, but it is at the court**'s** discretion to decide if such costs should be awarded.

vii. Factor 7—Recovery of Fees

As China has no discovery proceedings, patent litigation in China is generally less costly than litigation in the U.S., where extensive documentary discovery and oral depositions are typical. Litigants in China also have a fair chance to recover reasonable expenses, including attorney fees and court fees so long as sufficient evidence is presented to the court.

---

153. *See* Wuhan Jingyuan Envtl. Eng'g Co. v. Fuji Chem. Water Indus. Co. and Huayang Electric Indus. Co., Civil No. 8 (Supreme People's Court–Civil Division 2008), *available at* http://shzcfy.gov.cn/detail.jhtml?id=168132.

Where the patentee claims the payment for its reasonable expenses incurred to cease the infringement, the people**'s** court may calculate it separate from and in addition to the amount of compensation determined in accordance with the Chinese Patent Law.[154] In one case involving infringement upon a utility model patent, the Supreme People**'s** Court discretionarily awarded RMB 60,000 (approximately $8,500 U.S.), covering the estimated attorney fees, notarization fees, and cost of sample infringing products, despite the fact that the plaintiff did not submit any evidence of the estimated attorney fees.[155]

b. Opportunity for Defendant-Initiated Litigation

Jurisdictional Challenge. In China, defendants of patent infringement proceedings commonly contest the jurisdiction of the court by filing a jurisdictional challenge, particularly because defendants are given a relatively short period of time to submit a defense brief once the civil complaint has been served (15 days for a domestic party and 30 days for a foreign party from the date of service). When a defendant files a jurisdictional challenge, the exchange of evidence of the main proceedings will normally be postponed until after the jurisdiction issue is resolved, subject to negotiation by the parties. In the rare instances when a jurisdictional challenge is granted, the case will be transferred to another court with jurisdiction over the patent infringement dispute. Even further, the court's ruling on the jurisdictional challenge may be appealed to the second-instance court—the Intellectual Property Appeals Tribunal of

154. Chinese Patent Law, Supreme People's Court on Issues Concerning Applicable Laws to the Trial of Patent Controversies, Art. 71, 2020 Amendment.

155. *See* Wuxi Guowei Ceramic Elec. Appliance Co. v. Changshu Linzhi Elec. Heating Components Co., Civil Judgment No. 111 (China Supreme People's Court–Civil Division 2018).

the Supreme People's Court for invention and utility model patent cases; and the provincial High People's Court for design patent cases. Regardless of the result of a jurisdictional challenge, instituting such proceedings may extend the time for preparing the defense by three to four months. Nevertheless, defendants should be careful in making a jurisdictional challenge, because one that is determined to have been made with no proper and reasonable grounds could be perceived by Chinese courts to be in bad faith, which may adversely impact the patent infringement proceedings.

Declaratory Judgment. An accused party noticed of alleged patent infringement may seek a declaratory judgment of noninfringement if the party can show a legal interest in such adjudication. As in the U.S., defendants often use declaratory judgment actions to select a court that the party perceives as defendant friendly. Under Chinese law, three threshold requirements have to be met before courts can accept a noninfringement declaration claim: (i) a patentee gives a warning of patent infringement to another person; (ii) the person warned or an interested person sends a written reminder asking the patentee to exercise its right to sue; and (iii) the patentee neither withdraws the warning nor files a lawsuit within one month after receipt of the written reminder or within two months after issuing the written reminder.[156] In 2020, the Intellectual Property Tribunal of the Supreme People's Court recognized that an administrative complaint against the end user constitutes a claim of patent infringement against the

156. *See Analysing non-infringement declaration litigation in China*, MANAGING IP (Apr. 16, 2020), https://www.managingip.com/article/b1l3w2jsmw19zf/analysing-noninfringement-declaration-litigation-in-china.

manufacturer, enabling the manufacturer to commence a declaratory judgment action.[157]

Invalidation. China has a bifurcated patent system that allows parallel infringement and invalidation proceedings. An accused party of an infringement proceeding may commence invalidity challenges against a patent before the CNIPA, which will first be decided by the Patent Re-Examination Board of the CNIPA and can be appealed to the Beijing IP Court before appeal to the IP Appeals Tribunal of the Supreme People's Court. The grounds for filing an invalidity challenge include the lack of novelty, lack of inventiveness, lack of enablement, insufficient disclosure of written description, ineligible statutory subject matter, and double patenting. According to the CNIPA Annual Report, there were 7,095 invalidation cases accepted for 2022.[158] Of those proceedings, 1,431 cases were related to invention patents, 3,156 cases related to utility model patents, and 2,508 cases related to design patents.[159] The same Annual Report also notes that a total of 7,879 invalidation cases were successfully closed for the year 2022, suggesting a 11.5 percent increase as compared to 2021.[160]

157. *Id.* (discussing VMI Netherlands v. Safe-Run Huachen Mach. (Suzhou) Co., No. 5 (China Supreme People's Court–Intellectual Property Tribunal 2020), http://gongbao.court.gov.cn/Details/2bb16202c8444e985800ef7220e630.html.

158. *See 2022 Annual Report of the State Intellectual Property Office*, CHINA NAT'L INTELLECTUAL PROP. ADMIN. (Jun. 5, 2023), https://www.cnipa.gov.cn/art/2023/6/5/art_3249_185538.html.

159. *Id*.

160. *Id.*

c. Current Developments in Patent Litigation in China

In June 2021, the fourth amended Patent Law of the People's Republic of China came into effect. This amendment has substantially strengthened the patent enforcement system by introducing certain pro-patentee measures that are likely to motivate patentees to enforce their patent rights before Chinese courts. For instance, this amendment (i) increased the statutory damages minimum amount from RMB 10,000 to RMB 30,000 and maximum amount from RMB 1 million to RMB 5 million, and introduced punitive damages of up to five times the amount of compensation ascertained by court; (ii) shifted the burden of proving damages in patent infringement actions to the accused party by requiring the accused party to submit financial records and materials to evidence gains; (iii) enabled the CNIPA to determine patent infringement disputes of significant national impact; (iv) expanded the scope of protection over design patents (particularly on subject matter) and extended their term of protection; (v) codified presuit injunction, evidence preservation, and property preservation against accused parties; and (vi) extended the statutory limitation period for instating an action against patent infringement from two years to three years.[161]

According to the China Intellectual Property Rights Protection Report 2022 issued by the CNIPA, there were around

161. *See* National People's Congress of the People's Republic of China, Decision of the Standing Committee of the National People's Congress on Amending the Patent Law of the People's Republic of China, Order No. 55 of the President of the Peoples Republic of China (Oct. 17, 2020), http://en.npc.gov.cn.cdurl.cn/2020-10/17/c_674693.htm.

38,970 first-instance patent cases in 2022.[162] Given the recent amendment to the Chinese Patent Law and the emphasis on new creations in the Five-Year Plan (2021-25) of the State—particularly the Five-Year Plan Notice of the National Intellectual Property Protection and Utilization Plan released on October 28, 2021, which set a target of increasing the number of invention patents registered by 2025[163]—it is expected that the number of patent registrations and patent enforcement in China before Chinese courts will continue to increase in the next five to ten years.

162. *See The status of intellectual property protection in China in 2022*, CHINA NAT'L INTELLECTUAL PROP. ADMIN. (June 30, 2023), https://www.cnipa.gov.cn/art/2023/6/30/art_91_186011.html.

163. *See* The State Council issuance of the "14th Five-Year Plan" Notice of the National Plan for the Protection and Use of Intellectual Property Rights, STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA (Oct. 9, 2021), http://www.gov.cn/zhengce/zhengceku/2021-10/28/content_5647274.htm.

Moving the Law Forward in a Reasoned & Just Way