Selected Recent Sedona Conference® Working Group Series™ Publications
(May 2024)

The following publications are free for individual download from The Sedona Conference web site at https://thesedonaconference.org/publications. Registration is not required, but entering your Sedona Conference website username and password will speed up the download process, especially if multiple publications are desired. Reprint of any publication for more than personal use is restricted.

In keeping with The Sedona Conference's nonpartisan mission of moving the law forward in a reasoned and just way, each publication represents the consensus of the issuing Working Group, reached after initial drafting by a balanced team representing the major points of view on the topic, internal review by the full Working Group membership, dialogue at one or more Working Group meetings, and finally a public comment period (the most recent listings may still be in public comment phase). Each publication is described briefly in the following pages, with a link to the full publication at the end of each entry. The link will take you to a "download page," where all prior editions of this publication are listed and where any subsequent updates can be found, so you'll always be up to date.

Speakers on each of these topics are available for professional organizations, law schools, bar associations, judicial education programs, and other groups. No honoraria are required, although donations are gratefully accepted. Generally, a qualified member of the drafting or editorial team can be located close to your event to minimize travel costs. Please address speaking or reprint inquiries to info@sedonaconference.org.

Electronic Discovery

- The Sedona Principles, Third Edition (October 2017)
- The Sedona Canada Principles Addressing Electronic Discovery, Third Edition (January 2022)
- The Sedona Conference Commentary on Privilege Logs (May 2024)
- The Sedona Conference Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control" (February 2024)
- The Sedona Conference TAR Case Law Primer, Second Edition, (May 2023)
- The Sedona Conference Primer on Managing Electronic Discovery in Small Cases, (May 2023)
- The Sedona Conference Commentary on Managing International Legal Holds, (May 2023)

- The Sedona Conference Commentary on the Need for Guidance and Uniformity in Filing ESI and Records Under Seal (February 2022)
- The Sedona Conference Primer on Crafting eDiscovery Requests with "Reasonable Particularity" (January 2022)
- The Sedona Conference Commentary on the Effective Use of Federal Rule of Evidence 502(d) Orders (August 2021)
- The Sedona Conference Commentary on Ephemeral Messaging (June 2021)
- The Sedona Conference Commentary on ESI Evidence & Admissibility, Second Edition (October 2020)
- The Sedona Conference Commentary on Rule 45 Subpoenas to Non-Parties, Second Edition (October 2020)
- The Sedona Conference Cooperation Proclamation: Resources for the Judiciary, Third Edition (June 2020)
- The Sedona Conference Glossary, 5th Edition (February 2020)
- The Sedona Conference Commentary on Legal Holds, Second Edition: The Trigger & The Process (June 2019)
- The Sedona Conference Primer on Social Media, Second Edition (February 2019)
- The Sedona Canada Commentary on Discovery of Social Media (September 2021)
- The Sedona Conference Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations (May 2018)
- The Sedona Conference Federal Rule of Civil Procedure 34(b)(2) Primer: Practice Pointers for Responding to Discovery Requests (March 2018)
- The Sedona Conference Commentary on Proportionality in Electronic Discovery (May 2017)
- The Sedona Conference Guidance for the Selection of Electronic Discovery Providers (April 2017)

Information Governance

- The Sedona Conference Commentary on Information Governance, Second Edition (April 2019)
- The Sedona Conference Commentary on Defensible Disposition (April 2019)

Data Security and Privacy

- The Sedona Conference U.S. Biometric Systems Privacy Primer

- The Sedona Conference Commentary on Proposed Model Data Breach Notification Law, Public Comment Version (May 2023)
- The Sedona Conference Commentary on Quantifying Violations under U.S. Privacy Laws (July 2021)
- The Sedona Conference Commentary on a Reasonable Security Test (February 2021)
- The Sedona Conference Commentary on the Enforceability in U.S. Courts of Orders and Judgments Entered under GDPR (January 2021)
- The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers: Principles and Guidelines (August 2020)
- The Sedona Conference Commentary on Law Firm Data Security (July 2020)
- The Sedona Conference Incident Response Guide (January 2020)
- The Sedona Conference Commentary on Application of Attorney-Client Privilege and Work-Product Protection to Documents and Communications Generated in the Cybersecurity Context (November 2019)
- The Sedona Conference Commentary on Data Privacy and Security Issues in Mergers & Acquisitions Practice (May 2019)
- The Sedona Conference Data Privacy Primer (January 2018)

Cross-Border Data Transfers

- The Sedona Conference Commentary on Cross-Border Discovery in U.S. Patent and Trade Secret Cases (July 2023)
- The Sedona Conference Commentary on Cross-Border Privilege Issues (July 2022)
- The Sedona Conference Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders (April 2020)
- The Sedona Conference International Investigations Principles (May 2018)
- The Sedona Conference International Litigation Principles on Discovery, Disclosure & Data Protection in Civil Litigation, Transitional Edition (January 2017)
- The Sedona Conference Practical In-House Approaches for Cross-Border Discovery and Data Protection (June 2016)

Trade Secrets

- The Sedona Conference Commentary on Monetary Remedies in Trade Secret Litigation (July 2023)
- The Sedona Conference Commentary on the Governance and Management of Trade Secrets (July 2023)

- The Sedona Conference Framework for Analysis on Trade Secrets Across International Borders: Extra Territorial Reach (June 2022)
- The Sedona Conference Commentary on Protecting Trade Secrets in Litigation About Them (March 2022)
- The Sedona Conference Commentary on Protecting Trade Secrets Throughout The Employment Life Cycle (March 2022)
- The Sedona Conference Commentary on Equitable Remedies in Trade Secret Litigation (March 2022)
- The Sedona Conference Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases (October 2020)

Patent Litigation

- The Sedona Conference Commentary on Patent Litigation Best Practices: Streamlining Lower-Value Patent Cases (July 2023)
- The Sedona Conference Framework for Analysis for the Efficient Resolution of Disputes before the Forthcoming European Unified Patent Court (May 2023)
- The Sedona Conference Framework for Analysis of Standard-Essential Patent (SEP) and Fair, Reasonable, and Non-Discriminatory (FRAND) Licensing and Royalty Issues (January 2023)
- The Sedona Conference Executive Summary: Working Group 10 on Patent Litigation Best Practices & Working Group 9 on Patent Damages and Remedies

Appendix

- The Sedona Conference Cooperation Proclamation

The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production (October 2017)

The Third Edition of *The Sedona Principles* is a project started in 2002 by The Sedona Conference Working Group on Electronic Document Retention & Production (WG1). From its inception, *The Sedona Principles* was intended to serve as best practices, recommendations, and principles for addressing electronically stored information (ESI) issues in disputes—whether in federal or state court, and whether during or before the commencement of litigation. Throughout its 15-year evolution, *The Sedona Principles* has been recognized as a foundational guide for attorneys and judges confronting the novel challenges of eDiscovery. The Third Edition reflects the development of electronic discovery practice over the past decade and the 2015 amendments to the Federal Rules of Civil Procedure.

The Sedona Principles, Third Edition presents fourteen practical Principles for addressing Electronic Document Production:

Principle 1: Electronically stored information is generally subject to the same preservation and discovery requirements as other relevant information.

Principle 2: When balancing the cost, burden, and need for electronically stored information, courts and parties should apply the proportionality standard embodied in Fed. R. Civ. P. 26(b)(1) and its state equivalents, which requires consideration of 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.

Principle 3: As soon as practicable, parties should confer and seek to reach agreement regarding the preservation and production of electronically stored information.

Principle 4: Discovery requests for electronically stored information should be as specific as possible; responses and objections to discovery should disclose the scope and limits of the production.

Principle 5: The obligation to preserve electronically stored information requires reasonable and good faith efforts to retain information that is expected to be relevant to claims or defenses in reasonably anticipated or pending litigation. However, it is unreasonable to expect parties to take every conceivable step or disproportionate steps to preserve each instance of relevant electronically stored information.

Principle 6: Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information.

Principle 7: The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronically stored information were inadequate.

Principle 8: The primary sources of electronically stored information to be preserved and produced should be those readily accessible in the ordinary course. Only when electronically stored information is not available through such primary sources should parties move down a continuum of less accessible sources until the information requested to be preserved or produced is no longer proportional.

Principle 9: Absent a showing of special need and relevance, a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual electronically stored information.

Principle 10: Parties should take reasonable steps to safeguard electronically stored information, the disclosure or dissemination of which is subject to privileges, work product protections, privacy obligations, or other legally enforceable restrictions.

Principle 11: A responding party may satisfy its good faith obligations to preserve and produce relevant electronically stored information by using technology and processes, such as sampling, searching, or the use of selection criteria.

Principle 12: The production of electronically stored information should be made in the form or forms in which it is ordinarily maintained or that is reasonably usable given the nature of the electronically stored information and the proportional needs of the case.

Principle 13: The costs of preserving and producing relevant and proportionate electronically stored information ordinarily should be borne by the responding party.

Principle 14: The breach of a duty to preserve electronically stored information may be addressed by remedial measures, sanctions, or both: remedial measures are appropriate to cure prejudice; sanctions are appropriate only if a party acted with intent to deprive another party of the use of relevant electronically stored information.

The full text of *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, is available free for individual download

from The Sedona Conference website at
https://thesedonaconference.org/publication/The_Sedona_Principles.

The Sedona Canada Principles
Addressing Electronic Discovery, Third Edition
(January 2022)

When the first edition of the *Sedona Canada Principles* was published in 2008, it was immediately recognized by federal courts as an authoritative source of guidance in the area of electronic discovery for Canadian practitioners and was explicitly referenced in the Ontario Rules of Civil Procedure and practice directives that went into effect in January 2010. The *Second Edition of the Principles* was published in November 2015. Since that time, there have been significant technological and societal changes that have changed how Canadian legal practitioners manage eDiscovery. This Third Edition addresses the interplay between eDiscovery and developing privacy regimes in Canada, and the role of information governance to facilitate eDiscovery. The update also incorporates updated commentary, illustrations, and the ever-growing body of case law that have impacted Canadian courts and litigators. Among the topics that have been newly examined are:

- the proliferation of new types of data sources, including ephemeral data and workplace collaboration tools;
- best practices for remote data collection;
- the use of artificial intelligence tools and other emerging technologies to process electronically stored information (ESI);
- the pros and cons of keyword searches
- cross-border privacy issues

Principle 1: Electronically stored information is discoverable.

Principle 2: In any proceeding, the parties should ensure that steps taken in the discovery process are proportionate, taking into account: (i) the nature and scope of the litigation; (ii) the importance and complexity of the issues and interests at stake and the amounts in controversy; (iii) the relevance of the available ESI; (iv) the importance of the ESI to the court's adjudication in a given case; and (v) the costs, burden, and delay that the discovery of the ESI may impose on the parties.

Principle 3: As soon as litigation is reasonably anticipated, parties must consider their obligation to take reasonable and good-faith steps to preserve potentially relevant electronically stored information.

Principle 4: Counsel and parties should cooperate in developing a joint discovery plan to address all aspects of discovery and should continue to cooperate throughout the discovery process, including the identification, preservation, collection, processing, review, and production of electronically stored information.

Principle 5: The parties should be prepared to produce relevant electronically stored information that is reasonably accessible in terms of cost and burden.

Principle 6: A party should not be required, absent agreement or a court order based on demonstrated need and relevance, to search for or collect deleted or residual electronically stored information that has been deleted in the ordinary course of business or within the framework of a reasonable information governance structure.

Principle 7: A party may use electronic tools and processes to satisfy its discovery obligations.

Principle 8: The parties should agree as early as possible in the litigation process on the scope, format, and organization of information to be exchanged.

Principle 9: During the discovery process, the parties should agree to or seek judicial direction as necessary on measures to protect privileges, privacy, trade secrets, and other confidential information relating to the production of electronically stored information.

Principle 10: During the discovery process, the parties should anticipate and respect the rules of the forum or jurisdiction in which the litigation takes place, while appreciating the impact any decisions may have in related proceedings in other forums or jurisdictions.

Principle 11: Sanctions may be appropriate where a party will be materially prejudiced by another party's failure to meet its discovery obligations with respect to electronically stored information.

Principle 12: The reasonable costs of all phases of discovery of electronically stored information should generally be borne by the party producing it. In limited circumstances, it may be appropriate for the parties to arrive at a different allocation of costs on an interim basis, by either agreement or court order.

The full text of *The Sedona Canada Principles Addressing Electronic Discovery, Third Edition*, Public Comment Version, is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/The_Sedona_Canada_Principles.

The Sedona Conference Commentary on Privilege Logs
(May 2024)

The Sedona Conference Commentary on Privilege Logs (*Commentary*) offers tools and strategies for both responding and requesting parties to mitigate the considerable burdens and competing interests that can be associated with privilege logs.

When a party withholds otherwise discoverable information based on attorney-client privilege, work-product doctrine, or some other protection, Federal Rule of Civil Procedure 26(b)(5)(A) requires that the party must (1) "expressly make the claim" and (2) describe the nature of the information in such a way that allows the receiving party to assess the claim. The Rule does not, however, specify *how* the responding party must satisfy it obligation.

The most common tool parties have used is a "traditional" privilege log, which is arguably the most detailed and thorough method of expressly describing the bases for withholding documents as privileged. Determining the Privilege Asserted and crafting a custom Privilege Narrative/Description requires analysis for each document and, depending on the complexity of the document, can take significant time to draft a defensible custom privilege description. The proliferation of ESI in discovery can result in the responding party withholding thousands of documents based on claims of privilege, and the time and cost incurred in the effort to form descriptive sentences for each entry on these voluminous logs can be burdensome. This *Commentary* provides options for how responding parties can reduce the burden of satisfying their obligations and how parties can engage in constructive discussions to minimize disputes.

The privilege logging process can also raise issues for the requesting party (i.e., the party receiving the privilege log). These issues typically relate to the amount and nature of information on the privilege log. Specifically, a privilege log with fewer details can impair the requesting party's ability to understand the assertion of privilege, leaving the party to guess as to whether (or not) privilege properly attaches to the withheld documents.

Not surprisingly, the competing interests—and countervailing burdens and rights—of requesting and responding parties in discovery can lead to disputes about how and when a responding party will substantiate its assertions of privilege, and if a privilege log is used, whether the form and content of that privilege log are sufficient.

This *Commentary* outlines how parties and, if necessary, the courts can cooperatively address the burdens associated with privilege logs. The primary conclusions and recommendations are as follows:

- The parties should address privilege log format, timing, and anticipated issues, as well as contemplate procedures for seeking court assistance in resolving any privilege disputes, early in their case to help reduce costly discovery disputes later.

- Parties should discuss whether certain categories of documents, such as communications between a client and its outside litigation counsel about the litigation after a complaint has been filed, can be excluded from a privilege log in the first instance.
- Parties should discuss whether a "metadata plus topic log," or another alternative format, should be employed in their case. This *Commentary* takes the position that a "metadata plus topic log" is a preferred format over the traditional privilege log because it generally is more effective in satisfying the requirements of Rule 26(b)(5) while also mitigating the burdens associated with narrative descriptions.
- Acknowledging that practical burdens exist in the privilege logging process does not mean that the responding party's legal burden of supporting its privilege claims should shift to the requesting party. Consistent with the Federal Rules, the onus is on the responding party to satisfy the requirements of Rule 26(b)(5) and not on the requesting party to justify why those requirements should be met.
- In keeping with *The Sedona Principles, Third Edition*, proportionality should be considered and applied to all aspects of discovery, including the preparation of privilege logs.

The *Commentary*'s appendices include examples of various privilege log formats along with sample documents that appear on the logs. The exemplar documents are useful tools for helping to understand terminology and illustrate different types of privilege logs, as well as provide a visual representation of the strengths and weaknesses of each type of privilege log.

The full text of *The Sedona Conference Commentary on Privilege Logs* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Privilege_Logs.

The Sedona Conference Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control" (February 2024)

Rule 34 and Rule 45 of the Federal Rules of Civil Procedure obligate a party responding to a document request or subpoena to produce "documents, electronically stored information, and tangible things" in that party's "possession, custody, or control." However, the Rules are silent on what "possession, custody, or control" means, and the case law is unclear and inconsistent. This inconsistency often leads to sanctions for unintended and uncontrollable circumstances. This Commentary is intended to provide practical, uniform and defensible guidelines regarding when a responding party should be deemed to have "possession, custody, or control" of documents and electronically stored information.

This Commentary introduces and explains five practical "Principles on Possession, Custody, or Control":

Principle 1	A responding party will be deemed to be in Rule 34 or Rule 45 "possession, custody, or control" of Documents and ESI when that party has actual possession or the legal right to obtain and produce the Documents and ESI on demand.
Principle 2	The party opposing the preservation or production of specifically requested Documents and ESI claimed to be outside its control, generally bears the burden of proving that it does not have actual possession or the legal right to obtain the requested Documents and ESI.
Principle 3(a)	When a challenge is raised about whether a responding party has Rule 34 or Rule 45 "possession, custody, or control" over Documents and ESI, the Court should apply modified "business judgment rule" factors that, if met, would allow certain, rebuttable presumptions in favor of the responding party.
Principle 3(b)	In order to overcome the presumptions of the modified business judgment rule, the requesting party bears the burden to show that the responding party's decisions concerning the location, format, media, hosting, and access to Documents and ESI lacked a good faith basis and were not reasonably related to the responding party's legitimate business interests.
Principle 4	Rule 34 and Rule 45 notions of "possession, custody, or control" should never be construed to override conflicting state or federal privacy or other statutory obligations, including foreign data protection laws.

Principle 5 If a party responding to a specifically tailored request for Documents or ESI (either prior to or during litigation) does not have actual possession or the legal right to obtain the Documents or ESI that are specifically requested by their adversary because they are in the "possession, custody, or control" of a third party, it should, in a reasonably timely manner, so notify the requesting party to enable the requesting party to obtain the Documents or ESI from the third party. If the responding party so notifies the requesting party, absent extraordinary circumstances, the responding party should not be sanctioned or otherwise held liable for the third party's failure to preserve the Documents or ESI.

This Commentary reflects the culmination of over three years of dialogue, review, public comment, and revision, and incorporates the collective expertise of a diverse group of lawyers and representatives of firms providing consulting and legal services to both requesting and responding parties in civil litigation.

The Sedona Conference TAR Case Law Primer, Second Edition, (May 2023)

The use of Technology Assisted Review (TAR) to search for electronically stored information (ESI) has become common practice in litigation. Courts routinely cite TAR's benefits and encourage its use. But with more frequent use of TAR and greater familiarity with TAR workflows, courts are now grappling with increasingly more complex TAR disputes than they dealt with when The Sedona Conference published the first edition of the *TAR Case Law Primer* in January 2017.

Case law has developed in the intervening years to address issues such as TAR methodologies, metrics, and validation. *The Tar Case Law Primer, Second Edition* updates and replaces the First Edition, providing a comprehensive look at the cases that have substantively addressed TAR through December 31, 2022. It discusses how the technological shift from TAR 1.0 systems to TAR 2.0 (continuous active learning) has impacted the case law, spotlights key trends and issues relating to TAR, and summarizes the current state of the law and the open questions that remain.

As with the First Edition, the *Primer* does not recommend best practices or otherwise comment on the utility of TAR. It is intended to assist courts and practitioners in staying abreast of this evolving area of law and technology.

Section II addresses the history of judicial acceptance of TAR, beginning with *Da Silva Moore v. Publicis Groupe* in 2012. Section III discusses how courts have accepted the use of TAR when parties agree to its use, and how they have held parties to their prior agreements. Section IV examines the level of transparency and disclosure that courts expect in connection with TAR. Section V addresses issues related to TAR workflows, including search-term culling, recall thresholds, ESI orders and TAR protocols. Section VI discusses court-ordered ESI protocols in relation to a responding party's production decisions. Section VII examines the application of proportionality in relation to TAR; Section VII examines cost shifting; Section IX looks at TAR cases from foreign jurisdictions; and Section X examines the use of TAR in governmental investigations.

The full text of *The Sedona Conference Tar Case Law Primer, Second Edition* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/TAR_Case_Law_Primer.

The Sedona Conference Primer on Managing Electronic Discovery in Small Cases (May 2023)

"Small" cases—those matters involving smaller volumes or less complex varieties of electronically stored information (ESI), or in which the smaller stakes limit the time and money that can and should be spent on electronic discovery—are as varied as they are voluminous. Unlike larger cases where the financial or public policy stakes are higher, the cost and burden of employing the latest and greatest ESI preservation and production practices may not be necessarily proportional to the needs of a small case or consistent with meeting the mandate of Federal Rule of Civil Procedure 1: The just, speedy, and inexpensive determination of every action and proceeding.

The Sedona Conference Primer on Managing Electronic Discovery in Small Cases offers best practices and practical guidance tailored to the particularities of these "smaller" cases. In the interest of the underlying concept of proportionality—tailoring eDiscovery efforts to fit the circumstances of the case and the resources at hand—some of the guidance provided may diverge from what The Sedona Conference recommends for large, more complex cases. But just as in larger cases, the *Primer* acknowledges and reinforces the guiding principles of proportionality, cooperation, and communication in efficiently and cost-effectively managing discovery.

The *Primer* explores what constitutes a "small case," addresses the proportionality considerations that may justify creative or simpler approaches for some aspects of discovery in small cases, and offers pragmatic examples of how The Sedona Principles might be applied to conducting discovery in the most efficient and cost-effective manner. While there can be no one-size-fits-all approach, the *Primer* provides practical guidance for practitioners and the bench on all aspects of the discovery process, including early client engagement, custodian interviews, preservation and legal holds, Bring Your Own Device issues, ESI protocols, privilege assertions, motion practice, evidence admissibility and authentication, and the efficient use of technology.

The *Primer* concludes with an appendix that identifies some low-cost or no-cost tools and technologies that can help meet the needs of small cases when on a tight budget.

The full text of *The Sedona Conference Primer on Managing Electronic Discovery in Small Cases* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Primer_on_Managing_Electronic_Discovery_in_Small_Cases.

The Sedona Conference
Commentary on Managing International Legal Holds
(May 2023)

The Sedona Conference Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6) developed the *Commentary on Managing International Legal Holds* ("*Commentary*") to expand upon Guideline 12 of The Sedona Conference *Commentary on Legal Holds, Second Edition: The Trigger & The Process* (which addresses the implications of preserving information located outside of the United States) by focusing on "international legal holds," defined as legal holds involving preservation obligations that cross international borders. The *Commentary* provides guidance and practice points for implementing international legal holds while at the same time complying with potentially conflicting international data protection laws and regulations.

Section I is the introduction to the *Commentary.* Section II of the *Commentary* provides an overview of preservation and international data protection requirements. Section III sets out practice points to help organizations and counsel navigate international legal holds that may potentially conflict with international data protection laws.

The practice points outlined in Section III are as follows:

- **Practice Point 1:** Determine Whether the Preservation of Personal Data Is Necessary, and Then Determine Whether a Data Protection Law Applies
- **Practice Point 2:** Apply the Data Protection Law's Guiding Principles for Processing Personal Information to Every Preservation Step or Process
- **Practice Point 3:** Document the Lawful Basis for Preservation and Preservation Steps Taken Thereafter
- **Practice Point 4:** Take Steps to Minimize the Scope of Preserved Information
- **Practice Point 5:** Consider Involving Data Protection Officers, Supervisory Authorities, or Work Councils
- **Practice Point 6**: Communicate Clearly with Data Subjects, Advising What Materials the Organization is Preserving, and What Steps Will be Taken as to Personal Information
- **Practice Point 7**: Make Sure Legal Hold Notices are Translated in Accordance with Local Law

- **Practice Point 8**: Reevaluate and Release Legal Holds and Dispose of Information When No Longer Needed

The full text of *The Sedona Conference Commentary on Managing International Legal Holds* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Managing_International_Legal_Holds.

The Sedona Conference Commentary on the Need for Guidance and Uniformity in Filing ESI and Records Under Seal
(February 2022)

The intent of the *Commentary on the Need for Guidance and Uniformity in Filing ESI and Record Under Seal* ("*Commentary*") is to minimize the burden on litigants and courts created by the lack of uniformity in United States district court procedures for sealing confidential documents and electronically stored information (ESI).

For example, the district courts have different rules governing when a motion to seal must be filed, whether Electronic Case Filing ("ECF") can, should, or must be used, and how long sealed ESI and records will remain sealed. Moreover, the *Commentary* recognizes an inequity inherent in the sealing processes used by nearly every court. Namely, that the burden to seal ESI and records is placed on the party that did not designate such material as confidential, and in many instances, disagrees with the confidential designation and hence the request to seal. This results in an impracticable situation in which, by application of local sealing rules, the filing party must file a motion to seal documents that it may actually oppose. As a result, the filed motion to seal is oftentimes perfunctory and lacking in meaningful content.

So that the court can properly weigh whether the confidential documents meet the requirements to be sealed, this *Commentary* posits that it should be the designating party's burden to file a declaration in support of sealing, because the designating party is uniquely situated and appropriately motivated to describe the nature and basis of each confidential document. Only upon such proper foundation can the court determine whether the documents or information at issue should be sealed from public view.

The *Commentary* includes a Proposed Model Rule designed to make the process for sealing confidential ESI and records uniform across all federal jurisdictions. The Proposed Model Rule does not provide any guidelines or guidance for what ESI is properly sealed or redacted. Rather, the *Commentary* and Proposed Model Rule are intended to provide guidance as to the *procedures* for sealing ESI and records, as well as suggestions to avoid potential pitfalls that may be encountered when moving to seal ESI and records.

The Proposed Model Rule also addresses other inconsistencies and differences between the local sealing rules, including setting a uniform and reasonable time frame to file a motion to seal, proper notice to be provided to non-parties whose confidential documents are subject to a Notice of Proposed Sealed Record, and how sealed and redacted records are to be filed by the parties and disposed of by the court.

The changes proposed in this *Commentary* are designed both to bring uniformity to the process of filing under seal and to create a fair and efficient method to deal with the sealing and redacting of ESI, so that the parties can focus on the litigation while conserving the resources of the court.

The full text of *The Sedona Conference Commentary on the Need for Guidance and Uniformity in Filing ESI and Records Under Seal* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Need_for_ Uniformity_in_Filing_ESI_Under_Seal.pdf_.

The Sedona Conference Primer on Crafting eDiscovery Requests with "Reasonable Particularity," (January 2022)

For years, courts and parties have struggled with the issue of boilerplate discovery that provides only a vague picture of information being requested or produced, clogging the courts and increasing litigation costs. After the Rules Committee targeted the problem of boilerplate objections in the 2015 Amendments to the Federal Rules of Civil Procedure, those amendments became the focus of court opinions and industry guidance, including the Sedona Conference *Federal Rule of Civil Procedure 34(b)(2) Primer: Practice Pointers for Responding to Discovery Requests*, which was published in 2018. The focus on nonspecific objections also shed light on an opposing problem: The lack of precision in discovery *requests*.

Federal Rule of Civil Procedure 34(b) requires that discovery requests "describe with reasonable particularity" the information being sought. Rule 26(b) limits all discovery to information that is relevant and proportional to the needs of the case. And Rule 26(g) requires counsel to certify that every discovery request is "neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action." Despite these Rules, vague and overbroad discovery requests have continued.

The Sedona Conference Primer on Crafting eDiscovery Requests with "Reasonable Particularity" ('*Primer*') explores the origins of the "reasonable particularity" requirement, as well as the evolving case law addressing the standard. Drafting requests with "reasonable particularity" requires a heightened focus on the specific needs of the case. This *Primer* provides practical guidance on how to better target discovery and presents practice pointers for drafting requests for production in compliance with Rule 34(b)(1). It is hoped that the guidance provided in this *Primer*, in tandem with the *Rule 34(b)(2) Primer*, will result in more efficient discovery, reduced costs, and decreased court involvement in discovery disputes.

The full text of *The Sedona Conference Primer on Drafting eDiscovery Requests with "Reasonable Particularity*" is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Primer_on_Crafting_eDiscovery_Requests_with_Reasonable_Particularity.

The Sedona Conference Commentary on the Effective Use of Federal Rule of Evidence 502(d) Orders
(August 2021)

Federal Rule of Evidence 502 governs what happens when there is a disclosure of communication or information covered by the attorney-client privilege or work-product protection. Congress adopted the Rule in 2008 for two primary reasons. First, to address the "widespread complaint" that litigation costs related to the protection of privilege have become "prohibitive." Second, to "provide a party with . . . predictability that is needed to allow the party to plan in advance to limit the prohibitive costs of privilege and work-product review and retention.''

Rule 502 attempts to accomplish these goals primarily through Rule 502(d). Rule 502(d) permits parties to enter into a court order preventing waiver for privileged documents produced in the proceeding.

The Sedona Conference's consistent position is that parties should collectively seek entry of a Rule 502(d) non-waiver order. In practice, however, Rule 502(d) orders have been underutilized in federal litigation, in part because of a lack of understanding regarding the Rule's potential benefits, and also due to certain challenges with the use of such orders, such as through excessive clawback requests.

This *Commentary* encourages more robust use of Rule 502(d) orders by highlighting the benefits of 502(d) orders, clarifying confusion regarding the Rule's protections and limits, and suggesting methods to deal with the potential challenges of such orders. The publication also contains three appendices: Appendix A contains "model" language for a proposed Rule 502(d) order; Appendix B contains a list of U.S. district courts that have promulgated model Rule 502(d) orders as of the date of this publication; and Appendix C reproduces the Explanatory Note to Federal Rule of Evidence 502.

By both emphasizing how practitioners and jurists may benefit from using Rule 502(d) orders and by noting issues that could otherwise impede their effectiveness, it is hoped that this *Commentary* results in more widespread use of Rule 502(d) orders.

The full text of *The Sedona Conference Commentary on the Effective Use of Federal Rule of Evidence 502(d) Orders* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Effective_Use_of_FRE_502d_Orders.

The Sedona Conference Commentary on Ephemeral Messaging (July 2021)

The Sedona Conference Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6) developed the *Commentary on Ephemeral Messaging* ("*Commentary*") to address the tension between (a) the role of ephemeral messaging in complying with cross-border data protection mandates and information governance best practices to minimize data and (b) meeting law enforcement and regulatory requirements to capture communications, and litigation obligations to preserve data.

Section I is the introduction to the *Commentary.* Section II of the *Commentary* defines the nature and scope of ephemeral messaging, while Section III provides a detailed sketch of the tension and competing demands facing organizations that wish to use these tools.

Section IV encompasses a series of guidelines that provide direction to organizations on how to navigate the landscape of uncertainty surrounding the use of ephemeral messaging. The guidelines also offer recommendations to regulators and judges for evaluating good-faith uses of corporate ephemeral messaging. The guidelines are as follows:

- **Guideline One**: Regulators and Courts Should Recognize that Ephemeral Messaging May Advance Key Business Objectives
- **Guideline Two**: Organizations Should Take Affirmative Steps to Manage Ephemeral Messaging Risks
- **Guideline Three**: Organizations Should Make Informed Choices and Develop Comprehensive Use Policies for Ephemeral Messaging Applications
- **Guideline Four**: Regulators, Courts, and Organizations Should Consider Practical Approaches, Including Comity and Interest Balancing, to Resolve Cross-Jurisdictional Conflicts over Ephemeral Messaging
- **Guideline Five**: Reasonableness and Proportionality Should Govern Discovery Obligations Relating to Ephemeral Messaging Data in U.S. Litigation

The full text of The Sedona Conference *Commentary on Ephemeral Messaging* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Ephemeral_Messaging.

The Sedona Conference Commentary on ESI Evidence & Admissibility, Second Edition (October 2020)

The Sedona Conference Commentary on ESI Evidence & Admissibility, Second Edition addresses how the 2017 and 2019 changes to the Federal Rules of Evidence apply to the ever-changing landscape of technology and influence how parties manage electronically stored information (ESI).

The growth of eDiscovery reflects the increasing digitization of information in society, which also results in more relevant evidence being sourced from ESI. This phenomenon means that successful litigators must understand how to get ESI admitted into evidence, which is a different question than preserving or gathering it for discovery. This *Commentary* focuses specifically on that concern.

The First Edition of this *Commentary* was published in 2008. This Second Edition provides updated guidance that reflects the advances in technology and the amendments to the Federal Rules of Evidence, in particular FRE 803(16), 807, and 902(13) and (14). For example, the changes to Rule 803(16) address authentication of digital information that has been stored for more than 20 years, eliminating the concern that factual assertions made in massive volumes of ESI will be admissible for the truth simply because of their age. The new subsections (13) and (14) to Rule 902 provide for streamlined authentication of ESI and potentially eliminate the need to call a witness at trial to authenticate the evidence.

This *Commentary* is divided into three parts. First, there is a survey of the application of existing evidentiary rules and case law addressing the authenticity of ESI. Second, there are discussions about new issues and pitfalls, such as ephemeral data, blockchain, and artificial intelligence, looming on the horizon. Finally, there is practical guidance on admissibility and the use of ESI in depositions and in court.

The full text of *The Sedona Conference Commentary on ESI Evidence & Admissibility, Second Edition* is available for free individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_ESI_Evidence_and_Admissibility.

The Sedona Conference Commentary on Rule 45 Subpoenas to Non-Parties, Second Edition (October 2020)

Developments since the 2008 edition of The Sedona Conference *Commentary on Non-Party Production and Rule 45 Subpoenas* have led to significant revisions and additions now included in this *Second Edition*. Federal Rule of Civil Procedure 45 (Rule 45) was revised substantially in 2013. The 2015 amendments to the Federal Rules of Civil Procedure also impact Rule 45. The rise of cloud computing has put appreciable amounts of party data into the hands of non-parties, leading to increased use of Rule 45 subpoenas, in turn resulting in a significant growth of the case law under Rule 45. This *Second Edition* also incorporates the knowledge and guidance embodied in the updated Third Edition of *The Sedona Principles*.

The scope of this *Commentary* is limited to the use of Rule 45 subpoenas to obtain discovery from a non-party custodian of documents or electronically stored information (ESI). The Commentary does not address the use of Rule 45 subpoenas to (1) compel any person to appear and give testimony at a trial, hearing, or deposition, or (2) compel any person to appear and bring documents or ESI to a trial, hearing, or deposition.

Section II of this *Commentary* briefly explains the major revisions to Rule 45 made by the 2013 Rules amendments, as well as the effect of the 2015 Rules amendments.

Section III proposes an approach for determining whether a party has possession, custody, or control of information that may make a non-party subpoena inappropriate. In other words, if the non-party has possession or custody of electronically stored information (ESI) but a party retains control, the information should be obtained from the party under Rule 34, not from the non-party under Rule 45.

Section IV deals with preservation. A letter or similar request for the preservation of evidence generally does not create a non-party preservation obligation. In most cases, receipt of a properly served subpoena only obligates a non-party to take reasonable steps to produce the requested materials and does not obligate the non-party to initiate a formal legal hold process. Rather, the non-party's obligation is to ensure the requested information is not destroyed during the compliance period. However, once a non-party has complied with a subpoena by producing responsive documents and ESI, the non-party has no duty to preserve them.

Section V deals with the related concepts of sanctions under Rule 45(d)(1), cost shifting under Rule 45(d)(2)(B)(ii), and quashing or limiting the scope of a subpoena under Rule 45(d)(3), providing analysis of the now extensive case law under each of these approaches.

Finally, Section VI sets forth "Practice Pointers" for both parties and non-parties dealing with a Rule 45 subpoena.

The full text of *The Sedona Conference Commentary on Rule 45 Subpoenas to Non-Parties, Second Edition* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Non-Party_Production_and_Rule_45_Subpoenas.

The Sedona Conference Cooperation Proclamation: Resources for the Judiciary, Third Edition
(June 2020)

The Sedona Conference Cooperation Proclamation: Resources for the Judiciary, Third Edition ("Judicial Resources") provides state and federal trial judges with a comprehensive but easy-to-follow guide to eDiscovery case management, based on the precepts of *The Sedona Conference Cooperation Proclamation*.

This Third Edition is the first revision to the *Judicial Resources* since 2014 and reflects amendments to state and federal eDiscovery Rules, developments in case law, and advances in technology. It articulates a clear judicial philosophy of case management and resolution of discovery disputes and describes a framework by which federal and state judges can address and resolve discoveryissues that might arise in every stage of civil litigation.

The *Judicial Resources* addresses different styles of judicial management of electronically stored information (ESI) but suggests that active case management might be the most efficient means to resolve ESI-related disputes, assuming that the court has the means to do so. It also recognizes that not all civil actions are equal in the resources of the parties, the sophistication of counsel, or the actual amount in issue, so it encourages proportionality.

The *Judicial Resources* is structured around 20 stages of civil litigation when judicial management either proactively or in response to a request of the parties – is most appropriate or desirable. For each stage, the *Judicial Resources*:

- Identifies key issues that a judge is likely to face at each stage of litigation;
- Suggests strategies for case management or dispute resolution that encourage the parties,when possible, to reach a cooperative resolution at each stage;
- Provides exemplar court decisions or orders; and
- Recommends further readings on the issues presented at each stage that have been published by The Sedona Conference or are peer-reviewed.

The Judicial Resources is an ongoing project, edited by and for state and federal judges. Comments and suggestions are encouraged and can be submitted to resources@sedonaconference.org.

The full text of *The Sedona Conference Cooperation Proclamation: Resources for the Judiciary, Third Edition* is available for free individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Resources_for_the_Judiciary.

The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition
(February 2020)

This authoritative, 130-page Fifth Edition of *The Sedona Conference Glossary* defines nearly 800 eDiscovery terms and incorporates numerous additions and updates since publication of the Fourth Edition in 2014, reflecting the rapidly changing landscape of electronic discovery. It is a product of The Sedona Conference Technology Resource Panel (TRP) and includes significant input from the public since the First Edition of the *Glossary* was published in 2005.

The TRP has two components: a "User Group," whose members regularly negotiate and work with service providers; and a panel of service provider members, who have agreed to work with the User Group's output and who provide input along the way. The TRP was formed in the belief that a well-informed marketplace, speaking in the same language, will ultimately lead to reduced transaction costs for all parties, higher quality, and greater predictability.

The intent of the *Glossary* is to assist in the understanding of electronic discovery and electronic information management issues, allowing for more effective communication among all constituents in the eDiscovery process—clients, counsel, eDiscovery product and service providers, and the judiciary. We hope that the *Glossary* will serve as a useful and indispensable resource throughout the eDiscovery process, such as when discussing and negotiating the scope and conduct of eDiscovery in the spirit of cooperation.

The *Glossary* has been cited in law review articles and by state and federal courts in eDiscovery decisions. The Fifth Edition adds new terms, deletes outdated terms, and edits the definition of some terms to recognize evolving case law. There are additional citations for terms that have been relied upon by the judiciary in published opinions.

The full text of *The Sedona Conference Glossary* is available free
for individual download from The Sedona Conference website at
https://thesedonaconference.org/publication/The_Sedona_Conference_Glossary.

The Sedona Conference Commentary on Legal Holds, Second Edition: The Trigger & The Process
(June 2019)

Information lies at the core of civil litigation and our civil discovery system. Accordingly, the law has developed rules regarding the way information should be treated in connection with litigation. One of the principal rules is that when an organization reasonably anticipates litigation (as either the initiator or the target of litigation), the organization has a duty to undertake reasonable actions to preserve paper documents, electronically stored information (ESI), and tangible items that are relevant to the parties' claims and defenses and proportional to the needs of the case. The same preservation principle applies when an investigation is reasonably anticipated. The use of a "legal hold" has become a common means by which organizations initiate meeting their preservation obligations.

This Commentary provides practical guidelines for determining (a) when the duty to preserve discoverable information arises, and (b) once that duty is triggered, what should be preserved and how the preservation process should be undertaken.

Guideline 1: A reasonable anticipation of litigation arises when an organization is on notice of a credible probability that it will become involved in litigation, seriously contemplates initiating litigation, or when it takes specific actions to commence litigation.

Guideline 2: Adopting and consistently following a policy governing an organization's preservation obligations are factors that may demonstrate reasonableness and good faith.

Guideline 3: Adopting a procedure for reporting information relating to possible litigation to a responsible decision maker may assist in demonstrating reasonableness and good faith.

Guideline 4: Determining whether litigation is or should be reasonably anticipated should be based on a good-faith and reasonable evaluation of relevant facts and circumstances.

Guideline 5: Evaluating an organization's preservation decisions should be based on the good faith and reasonableness of the decisions (including whether a legal hold is necessary and how it should be implemented) at the time they are made.

Guideline 6: Fulfilling the duty to preserve involves reasonable and good-faith efforts, taken as soon as is practicable and applied proportionately, to identify persons likely to have information relevant to the claims and defenses in the matter and, as necessary, notify them of their obligation to preserve that information.

Guideline 7: Factors that may be considered in determining the scope of information that should be preserved include the nature of the issues raised in the matter, the accessibility of the information, the probative value of the information, and the relative burdens and costs of the preservation effort.

Guideline 8: In circumstances where issuing a legal hold notice is appropriate, such a notice is most effective when the organization identifies the custodians and data stewards most likely to have discoverable information, and when the notice:

(a) communicates in a manner that assists persons in taking actions that are, in good faith, intended to be effective;

(b) is in an appropriate form, which may be written, and may be sent by email;

(c) provides information on how preservation is to be undertaken, and identifies individuals who can answer questions about preservation;

(d) includes a mechanism for the recipient to acknowledge that the notice has been received, read, and understood;

(e) addresses features of discoverable information systems that may make preservation of discoverable information more complex (e.g., auto delete functionality that should be suspended, or small sections of elaborate accounting or operational databases);

(f) is periodically reviewed and amended when necessary; and

(g) is followed up by periodic reminder notices, so the legal hold stays fresh in the minds of the recipients.

Guideline 9: An organization should consider documenting the procedure of implementing the legal hold in a specific case when appropriate.

Guideline 10: Compliance with a legal hold should be regularly monitored.

Guideline 11: Any legal hold process should include provisions for releasing the hold upon the termination of the duty to preserve, so that the organization can resume adherence to policies for managing information through its useful life cycle in the absence of a legal hold.

Guideline 12: An organization should be mindful of local data protection laws and regulations when initiating a legal hold and planning a legal hold policy outside of the United States.

The full text of *The Sedona Conference Commentary on Legal Holds, Second Edition: The Trigger & The Process* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Legal_Holds.

The Sedona Conference Primer on Social Media, Second Edition (February 2019)

Social media is ubiquitous throughout most of the world, with users numbering in the billions irrespective of age, geography, or socioeconomic status. Not only consumers, but also governments and businesses employ social media to communicate with their constituencies and target audiences. With so many individuals and organizations communicating through social media, it is increasingly becoming a subject of discovery in litigation and investigations. Lawyers must understand the different types of social media and the unique discovery issues they present so they can advise and assist their clients in properly preserving, collecting, producing, and requesting such information in discovery.

The Sedona Conference's Working Group 1 on Electronic Document Retention & Production (WG1) initially addressed these issues when it published the first edition of *The Sedona Conference Primer on Social Media* in December 2012. Since then, however, there has been a proliferation of new messaging technologies and business applications, in addition to major evolution in "traditional" social media platforms like Facebook, Twitter, and LinkedIn. There have also been significant developments in the law addressing social media and in the rules of discovery, evidence, and professional responsibility. Therefore, WG1 recognized a compelling need to update the *Primer* and draft this Second Edition.

After a brief introduction in Section I of the *Primer on Social Media, Second Edition*, Section II discusses traditional and emerging social media technologies and the discovery challenges that they present. Section III examines relevance and proportionality in the context of social media. It also explores preservation challenges, collection and search obligations, and the impact of the Stored Communications Act ("SCA"), together with review and production considerations. Section IV describes the impact of cross-border issues on social media discovery while Section V explores authentication issues. The *Primer* concludes in Section VI by analyzing ethical issues that lawyers should consider in connection with social media discovery.

The full text of *The Sedona Conference Primer on Social Media, Second Edition*
is available free for individual download from The Sedona Conference website at
https://thesedonaconference.org/publication/Primer_on_Social_Media

The Sedona Canada Commentary on Discovery of Social Media (September 2021)

Social media is ubiquitous throughout most of the world, with users numbering in the billions irrespective of age, geography, or socioeconomic status. Not only consumers, but also governments and businesses employ social media to communicate with their constituencies and target audiences. With so many individuals and organizations communicating through social media, it is increasingly becoming a subject of discovery in legal proceedings and investigations. Lawyers must understand the different types of social media and the unique discovery issues they present so they can advise and assist their clients in properly preserving, collecting, producing, and requesting such information in discovery.

The Sedona Canada Commentary on Discovery of Social Media builds on similar principles and guidelines regarding social media developed by the Sedona Conference Working Group 1 for the United States, including The Sedona Conference *Primer on Social Media*, first published in 2012 and updated in 2019. However, this *Commentary* focuses on the regulatory and practice requirements of the Canadian legal profession.

Section II of the *Commentary* discusses traditional and emerging social media technologies and the discovery challenges they present. Section III examines relevance and proportionality in the context of social media. It also explores preservation challenges, collection, and search obligations, together with review and production considerations. Section IV describes the impact of cross-border issues on social media discovery, and Section V explores authentication issues. The *Commentary* concludes in Section VI by analyzing ethical issues that lawyers should consider in connection with social media discovery.

The full text of *The Sedona Canada Commentary on Discovery of Social Media* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Sedona_Canada_Commentary_on_Discovery_of_Social_Media.

The Sedona Conference Commentary on BYOD
(May 2018)

More than ever before, organizations are permitting or encouraging workers to use their own personal devices to access, create, and manage the organization's information—often after hours and outside the office. This practice is commonly referred to as Bring Your Own Device or BYOD and is often accomplished through a BYOD program that includes formal or informal rules and guidelines. The *Commentary on BYOD* is designed to help organizations develop and implement workable—and legally defensible—BYOD policies and practices. The commentary also addresses how creating and storing an organization's information on devices owned by employees impacts the organization's discovery obligations.

The first two principles and related commentary address determining whether a BYOD program is the right choice for an organization, followed by basic information governance requirements for BYOD—security, privacy, accessibility, and disposition—from the perspective of both domestic and global organizations. The remaining principles and commentary address preparing for and responding to discovery obligations under the prevailing U.S. approach to discovery.

Principle 1: Organizations should consider their business needs and objectives, their legal rights and obligations, and the rights and expectations of their employees when deciding whether to allow, or even require, BYOD.

Principle 2: An organization's BYOD program should help achieve its business objectives while also protecting both business and personal information from unauthorized access, disclosure, and use.

Principle 3: Employee-owned devices that contain unique, relevant ESI should be considered sources for discovery.

Principle 4: An organization's BYOD policy and practices should minimize the storage of––and facilitate the preservation and collection of—unique, relevant ESI from BYOD devices.

Principle 5: Employee-owned devices that do not contain unique, relevant ESI need not be considered sources for discovery.

The full text of *The Sedona Conference Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_BYOD.

The Sedona Conference Federal Rule of Civil Procedure 34(b)(2) Primer: Practice Pointers for Responding to Discovery Requests (March 2018)

The December 2015 amendments to Federal Rule of Civil Procedure 34 were intended to address systemic problems in how discovery requests and responses traditionally were handled, and yet, despite numerous articles, training programs, and conferences about the changes, implementation of the changes has been mixed, at best. Amended Rule 34 encourages an evolving and iterative conversation between requesting and responding parties about what is being sought and what will be produced. This *Primer* seeks to normalize that concept and provide a framework for how those conversations may proceed.

The *Primer*, which is the result of several months of review and analysis by a diverse team of the Working Group on Electronic Document and Retention (WG1) members, is not intended to be the last word on how to implement the amendments, as there is no "correct" way to do so, and new ideas and best practices are emerging every day. Rather, the *Primer* gathers advice and observations from: (i) requesting and responding parties who have successfully implemented them and (ii) legal decisions interpreting the amended Rules, and offers practice pointers on how to comply with the amended Rules. Additionally, the *Primer* includes additional references: Appendix A summarizes a number of cases that have addressed the specificity of requests for production, and the specificity of responses and objections to requests for production. Appendix B lists standing orders, checklists, and pilot programs that address discovery requests, discovery responses, and guidelines for when and how parties should confer regarding requests and responses.

The full text of *The Sedona Conference Federal Rule of Civil Procedure 34(b)(2) Primer* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Federal_Rule_of_Civil_Procedure_34_Primer.

The Sedona Conference Commentary on Proportionality in Electronic Discovery (May 2017)

Achieving proportionality in civil discovery is critically important to securing the "just, speedy, and inexpensive resolution of civil disputes" as mandated by Federal Rule of Civil Procedure 1. This is the third iteration of *The Sedona Conference Commentary on Proportionality in Electronic Discovery*, a project started in 2010 by The Sedona Conference Working Group on Electronic Document Retention & Production (WG1), revised in 2013, and now updated to reflect the significant and evolving emphasis on proportionality under the 2015 amendments to the Federal Rules of Civil Procedure. This *Commentary* delineates reasonable guidance on the application of proportionality standards that should enable common sense discovery practices and further the objective of the rules.

This *Commentary* presents six practical Principles of Proportionality:

Principle 1: The burdens and costs of preserving relevant electronically stored information should be weighed against the potential value and uniqueness of the information when determining the appropriate scope of preservation.

Principle 2: Discovery should focus on the needs of the case and generally be obtained from the most convenient, least burdensome, and least expensive sources.

Principle 3: Undue burden, expense, or delay resulting from a party's action or inaction should be weighed against that party.

Principle 4: The application of proportionality should be based on information rather than speculation.

Principle 5: Nonmonetary factors should be considered in the proportionality analysis.

Principle 6: Technologies to reduce cost and burden should be considered in the proportionality analysis.

The full text of *The Sedona Conference Commentary on Proportionality in Electronic Discovery* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Proportionality_in_Electronic_Discovery

The Sedona Conference Guidance for the Selection of Electronic Discovery Providers (April 2017)

Guidance for the Selection of Electronic Discovery Providers is a product of The Sedona Conference Technology Resource Panel (TRP). The TRP is comprised of "users" of eDiscovery services (from defense and plaintiff firms, corporate law departments, and consulting firms) with input from eDiscovery providers who registered as TRP members to support this effort in response to an open invitation.

Although there is a trend toward industry consolidation amongst eDiscovery providers, the overall number of providers continues to increase along with the spectrum of services they offer. This is not surprising in light of the growing volume of electronically stored information (ESI), ever-evolving advancements in technology, increased emphasis on ESI in the rules of courts and case law, and the continuing increase in demand for a broader range of services.

The purpose of this publication is to provide guidance to law firm attorneys, legal department attorneys, and litigation support professionals who are tasked with the challenge of finding an appropriate eDiscovery service provider for each phase of the eDiscovery process. This guidance comes in the form of information, sample forms, and checklists designed to provoke thought and provide clarity around the considerations that should be taken into account when trying to identify the appropriate provider and solution(s) for your specific circumstances.

The full text of *The Sedona Conference Guidance for the Selection of Electronic Discovery Providers* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Selection_of_Electronic_Discovery_Vendors.

The Sedona Conference Commentary on Information Governance, Second Edition (April 2019)

Information is one of modern businesses' most important assets and with the proliferation of data it has become very challenging to balance the use of data against privacy and security concerns. In addition, there is no generally accepted framework or methodology to help organizations make decisions about information for the benefit of the organization as an organization rather than an individual department or function.

In 2014, The Sedona Conference published its first edition of the *Commentary on Information Governance* which recommended a top-down, overarching framework guided by the requirements and goals of all stakeholders that enables an organization to make decisions about information for the good of the overall organization and consistent with senior management's strategic directions. This Second Edition of the *Commentary on Information Governance* ("Second Edition") accounts for the changes and advances in technology and law over the past four years; underscores the role of IG as part of and complimentary to the business, rather than something separate that adds overhead; and emphasizes the costs of eDiscovery which should drive organizations to focus on IG on the front end, resulting in eDiscovery that is more efficient, less painful, and which allows the organization to reap additional benefits from a business perspective. Additionally, this Second Edition also incorporates the knowledge and guidance embodied in the new and updated Sedona commentaries since 2014 such as *The Sedona Principles, Third Edition* and The Sedona Conference *Principles and Commentary on Defensible Disposition*.

Download the Commentary for an expanded discussion of the following 11 Principles of Information Governance:

Principle 1: Organizations should consider implementing an Information Governance program to make coordinated, proactive decisions about information for the benefit of the overall organization that address information-related requirements and manage risks while optimizing value.

Principle 2: An Information Governance program should maintain sufficient independence from any particular department or division to ensure that decisions are made for the benefit of the overall organization.

Principle 3: All stakeholders' views/needs should be represented in an organization's Information Governance program.

Principle 4: The strategic objectives of an organization's Information Governance program should be based upon a comprehensive assessment of information-related practices, requirements, risks, and opportunities.

Principle 5: An Information Governance program should be established with the structure, direction, resources, and accountability to provide reasonable assurance that the program's objectives will be achieved.

Principle 6: The effective, timely, and consistent disposal of physical and electronic information that no longer needs to be retained should be a core component of any Information Governance program.

Principle 7: When Information Governance decisions require an organization to reconcile conflicting laws or obligations, the organization should act in good faith and give due respect to considerations such as data privacy, data protection, data security, records and information management (RIM), risk management, and sound business practices.

Principle 8: If an organization has acted in good faith in its attempt to reconcile conflicting laws and obligations, a court or other authority reviewing the organization's actions should do so under a standard of reasonableness according to the circumstances at the time such actions were taken.

Principle 9: An organization should consider reasonable measures to maintain the integrity and availability of long-term information assets throughout their intended useful life.

Principle 10: An organization should consider leveraging the power of new technologies in its Information Governance program.

Principle 11: An organization should periodically review and update its Information Governance program to ensure that it continues to meet the organization's needs as they evolve.

The full text of *The Sedona Conference Commentary on Information Governance, Second Edition* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Information_Governance.

The Sedona Conference Commentary on Defensible Disposition (April 2019)

The Sedona Conference *Principles and Commentary on Defensible Disposition* grew from Principle 6 of The Sedona Conference *Commentary on Information Governance* which advises that the effective, timely, and consistent disposal of physical and electronic information that no longer needs to be retained should be a core component of any Information Governance program. However, many organizations struggle with making and executing effective disposition decisions.

That struggle is often caused by many factors, including the incorrect belief that organizations will be forced to "defend" their disposition actions if they later become involved in litigation. Indeed, the phrase "defensible disposition" suggests that organizations have a duty to defend their information disposition actions.

While it is true that organizations must make "reasonable and good faith efforts to retain information that is relevant to claims or defenses," that duty to preserve information is not triggered until there is a "reasonably anticipated or pending litigation" or other legal demands for records. Another factor in the struggle toward effective disposition of information is the difficulty in appreciating how such disposition reduces costs and risks. Lastly, many organizations struggle with *how* to design and implement effective disposition as part of their overall Information Governance program.

These Principles and the associated Commentary aim to provide guidance to organizations and counsel on the adequate and proper disposition of information that is no longer subject to a legal hold and has exceeded the applicable legal, regulatory, and business retention requirements.

Principle 1: Absent a legal retention or preservation obligation, organizations may dispose of their information.

Principle 2: When designing and implementing an information disposition program, organizations should identify and manage the risks of over-retention.

Principle 3: Disposition should be based on Information Governance policies that reflect and harmonize with an organization's information, technological capabilities, and objectives.

The full text of *The Sedona Conference Commentary on Defensible Disposition* is available free for individual download from The Sedona Conference website at:
https://thesedonaconference.org/publication/Commentary_on_Defensible_Disposition.

The Sedona Conference
U.S. Biometric Systems Privacy Primer
(May 2024)

The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11) developed the *U.S. Biometric Systems Privacy Primer* ("*Primer*") to provide a general introduction to biometric systems and a summary of existing U.S. laws regulating the collection, use, and sharing of the biometric information these technologies collect.

The *Primer* is written as a resource for lawyers, judges, legislators, and other policymakers. It provides a general guide to the relationships among the technical, legal, and policy aspects of biometric systems—with a particular focus on privacy and related concerns these systems may raise.

Part I is the introduction to the *Primer.* Part II of the *Primer* provides an overview of biometric recognition systems (which include both identity verification and identification systems) by private organizations. Part III discusses biometric system benefits and drawbacks. Part IV details the U.S. biometric privacy legal landscape, focusing in particular on U.S. state biometric privacy laws. Part V identifies several general considerations organizations should consider when selecting or designing biometric recognition systems.

The full text of The Sedona Conference *U.S. Biometric Systems Privacy Primer*, is available free for individual download from The Sedona Conference website at

https://thesedonaconference.org/publication/Biometric_Systems_Privacy_Primer

The Sedona Conference Commentary on Proposed Model Data Breach Notification Law
(May 2023 Public Comment Version)

The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11) developed the *Commentary on Proposed Model Data Breach Notification Law* ("*Commentary*") to address two key problems with current data breach notification statutes—(1) the lack of uniformity among the laws and (2) the fact that most data breach notification letters do little to help consumers. The *Commentary* puts forth a model data breach notification law. The *Commentary* is intended to inform policy decisions at the U.S. federal or state levels as data breach statutes evolve. Even if a legislature declines to adopt all of the recommendations made in the *Commentary*, it may benefit from the analysis as to specific elements of the proposed model data breach notification law.

Section I is the introduction to the *Commentary*. Section II provides background on the topic. Section III provides analysis and discussion of current U.S. state data breach notification laws and the proposed model data breach notification law. Section IV sets forth the proposed model data breach notification law in its entirety.

The eight areas where the *Commentary* suggests current iterations of U.S. state data breach notification laws can be improved by greater uniformity and clarity are as follows:

- Definition of a security breach
- Definition of PII
- Definition of risk of harm
- Encryption, de-identification, and similar technologies
- Method and form of notification
- Timeline for notification
- Credit monitoring
- Notifying law enforcement and regulatory authorities

Proposed model language for each of these eight areas is included in the *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.

The full text of *The Sedona Conference Commentary on Proposed Model Data Breach Notification Law*, Public Comment Version, is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Proposed_Model_Data_Breach_Notification_Law

The Sedona Conference Commentary on Quantifying Violations under U.S. Privacy Laws (July 2021)

As data privacy receives more attention in the United States and elsewhere—and as new laws in the U.S. take shape and are enacted— The Sedona Conference Working Group on Data Security and Privacy Liability (WG11) recognizes that a consistent approach to quantifying violations under U.S. privacy laws could be helpful to impacted parties, courts, authorities, and practitioners, not to mention the general public. With various jurisdictions and enforcement authorities involved in current and future enforcement of such data privacy laws, however, consistency can be challenging to reach. With an eye towards consistency, WG11 hopes that The Sedona Conference *Commentary on Quantifying Violations under U.S. Privacy Laws* ("*Commentary*") will be of use to stakeholders in reaching a fair interpretation of the meaning of a "per violation" measure of damages.

The first section of this *Commentary* reviews at a high level the landscape of existing privacy laws in the United States, addresses certain ambiguities regarding the calculation of penalties and damages that may arise under such laws, and examines the way in which other somewhat analogous statutes have been enforced across the country. The second section examines possible ways in which violations of privacy laws could be quantified given statutory construction and existing case law. The last section endeavors to provide a useful test courts can use to evaluate the meaning of a "per violation" measure of damages in the context of data privacy violations in a way that benefits consumers and provides deterrent value to regulators but is fair and provides due process to potential violators.

The full text of *The Sedona Conference Commentary on Quantifying Violations under U.S. Privacy Laws* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Quantifying_Violations_under_US_Privacy_Laws.

The Sedona Conference Commentary on a Reasonable Security Test (February 2021)

The Sedona Conference Working Group on Data Security and Privacy Liability (WG11) developed this *Commentary* to address what "legal test" a court or other adjudicative body should apply in a situation where a party has, or is alleged to have, a legal obligation to provide "reasonable security" for personal information, and the issue is whether the party in question has met that legal obligation.

The *Commentary* proposes a reasonable security test that is designed to be consistent with models for determining "reasonableness" that have been used in various other contexts by courts, in legislative and regulatory oversight, and in information security control frameworks. All of these regimes use a form of risk analysis to balance cost and benefit. The proposed test provides a practical method for expressing cost/benefit analysis that can be applied in data security regulatory actions, to litigation, and to information security practitioners using their current evaluation techniques. The *Commentary* also explains how the analysis should apply in the data security context. Because the test is rooted in commonly held principles, the drafters believe it offers methods for deriving reasonableness that are familiar to all interested parties. But it should be noted that depending on their text, individual laws or rules that require reasonable security might require use of a different analysis.

The *Commentary* begins with a brief summary of the importance of having a test, the reasoning behind a cost/benefit approach for the test, and what issues the test does not address. Part I sets out the proposed test and the explanation of how it is applied. Part II provides review and analysis of existing resources that offer guidance on how "reasonable security" has been defined and applied to date and explains how they bear upon the test. It includes a summary review of statutes and regulations that require organizations to provide reasonable security with respect to personal information, decisions of courts and other administrative tribunals with respect to the same, applicable industry standards, and marketplace information. Following this discussion, the *Commentary* identifies those items that are not included in the proposed test (also referenced in the Introduction section) and concludes with a discussion regarding the importance of flexibility.

The full text of The Sedona Conference *Commentary on a Reasonable Security Test* is available free for individual download from The Sedona Conference website at

https://thesedonaconference.org/publication/Commentary_on_Reasonable_Security_Test.

The Sedona Conference Commentary on the Enforceability in U.S. Courts of Orders and Judgments Entered under GDPR (January 2021)

The Sedona Conference Working Group on Data Security and Privacy Liability (WG11) developed the *Commentary on the Enforceability in U.S. Courts of Orders and Judgments Entered under GDPR* ("*Commentary*") to evaluate the enforceability in a United States court of an order or judgment entered under the European Union (EU) General Data Protection Regulation (GDPR) by an EU court, or by an EU Member State supervisory authority, against a U.S.-based controller or processor. The goal of the *Commentary* is to provide guidance to stakeholders in the EU and in the U.S. on the factors—both legal and practical—that speak to the enforcement of GDPR mandates through U.S. legal proceedings.

Part I of the *Commentary* provides an overview of GDPR's extraterritorial scope under GDPR Article 3 and briefly examines how EU supervisory authorities have interpreted that provision since GDPR entered into force in May 2018.

Part II addresses the state of the law in the U.S. regarding the recognition and enforcement of foreign country orders and judgments. Some states have addressed the issue by adopting statutes, and others have relied on the common law. Each approach, however, relies on a set of common principles. Part II describes those principles, touching on questions about enforcement of private money judgments and injunctions as well as public orders prohibiting or mandating certain conduct or levying fines or other penalties for violations of foreign laws.

Building on that discussion of general principles, Parts III, IV, and V address how those general principles apply to claims by private plaintiffs (Part III) and claims by EU supervisory authorities (Part IV), and the potential defenses they create for U.S. defendants (Part V).

Finally, Part VI briefly addresses the ways that GDPR's requirements might be enforced other than through the direct enforcement of an existing EU order or judgment entered under GDPR.

The full text of *The Sedona Conference Commentary on the Enforceability in U.S. Courts of Orders and Judgments Entered under GDPR* is available free
for individual download from The Sedona Conference website at
https://thesedonaconference.org/publication/Enforceability_in_US_Courts_under_GDPR.

The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers: Principles and Guidelines
(August 2020)

Legal service providers (LSPs) and third-party service providers that assist them in their legal practice rely on various forms of technology to communicate, create, share, and store information in the course of business. Technology poses risks to privacy and information security, including the confidentiality of privileged communications. This *Commentary* sets out a framework for mitigating these risks.

The focus of the *Commentary* is on personal and confidential information (PCI). Personal information is any information about an identifiable individual, such as contact information, medical or financial information, or biometric identifiers such as an individual's voice recording. Confidential information may relate to individuals or legal entities and includes any information subject to a lawyer's duty of confidentiality or a class of privilege.

Ethical rules, statutes, regulations, and the common law all impose duties on lawyers, paralegals, and less directly, on much of the legal services industry, to safeguard PCI belonging to clients and third parties. Engagement agreements may also contain requirements about the safekeeping and handling of PCI. This *Commentary* suggests some prospective and remedial measures that LSPs should consider in order to meet or exceed these obligations.

The discussion in this *Commentary* is informed by the following guiding principles:

Principle 1: **Know the law**: LSPs should know the relevant law in order to identify, protect, and secure PCI they control in their practices.

Principle 2: **Understand the PCI you control**: LSPs should understand what PCI is, and know the types of PCI in their control.

Principle 3: **Assess risk**: LSPs should periodically conduct a risk assessment of the PCI within their control. The risk assessment should consider the PCI's sensitivity and vulnerability, and the harm that would result from its loss or disclosure.

Principle 4: **Develop policies and practices**: After completing a risk assessment, LSPs should develop and implement appropriate policies and practices to mitigate the risks identified in the risk assessment.

Principle 5: **Monitor regularly**: LSPs should monitor their operations on a regular basis for compliance with privacy and security policies and practices.

Principle 6: **Reassess**: LSPs should periodically reassess risks and update their privacy and information security policies and practices to address changing circumstances.

This *Commentary* is intended to help all LSPs—sole practitioners, law firms of all sizes, paralegals, law clerks, and legal support entities—determine which policies and practices are best suited for them. It aims to give practical guidance to LSPs by exploring "real-life" scenarios involving the loss of PCI, or the breach of security measures designed to protect it, commonly experienced in practice.

The full text of *The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers: Principles and Guidelines* is available free for individual download from The Sedona Conference website at
https://thesedonaconference.org/publication/Sedona_Canada_Commentary_on_Privacy_and_Information_Security.

The Sedona Conference Commentary on Law Firm Data Security (July 2020)

The Sedona Conference Working Group on Data Security and Privacy Liability (WG11) developed the *Commentary on Law Firm Data Security* ("*Commentary*") to identify ways that organizations and their law firms should approach and address organization expectations and firm capabilities regarding data security. The *Commentary* provides best practices focused on data security requirements that are meaningful considering the organization's obligation to protect the data, the type of data the organization is providing to the law firm, and the law firm's operating environment. In short, the *Commentary* intends to provide an effective road map for more efficient, effective communication to address data security issues and scenarios confronted by organizations and the law firms they engage.

While the *Commentary* may be of interest to other audiences, it is primarily directed toward two: first, to in-house counsel and an organization's technical personnel charged with ensuring that organizational service providers handle data securely; and second, to the law firm professionals and technical personnel overseeing and implementing data security at law firms.

The *Commentary* is organized into the following sections:

1. Common criteria and protocols for assessing data security at law firms
2. Considerations for how an organization should communicate with outside counsel about the security of the organization's data

The appendices of the *Commentary* include the following items that will be of particular practical benefit to organizations and law firms:

1. Model clauses for an engagement letter
2. Sample law firm questionnaire

The full text of *The Sedona Conference Commentary on Law Firm Data Security,* Public Comment Version, is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Law_Firm_Data_Security.

The Sedona Conference Incident Response Guide
(January 2020)

The Sedona Conference Working Group on Data Security and Privacy Liability (WG11) developed the *Incident Response Guide* to provide a comprehensive but practical guide to help practitioners and organizations deal with the multitude of legal, technical, and policy issues that arise whenever a data breach occurs. The *Incident Response Guide* is intended to help organizations prepare and implement an incident response plan and, more generally, to understand the information that drives the development of such a plan.

Nothing contained in the *Incident Response Guide* is intended to establish a legal standard or a yard-stick against which to measure compliance with legal obligations. A reader should neither assume that following the guidance in the *Incident Response Guide* will insulate it from potential liability, nor that failure to adhere to the guidance will give rise to liability. Rather, the purpose is to identify in detail issues that should be considered when addressing the preparation and implementation of an incident response that is suitable to his or her organization.

The target audience for the *Incident Response Guide* is small- to medium-sized organizations, which will not have unlimited resources to devote to incident responses. However, it is anticipated that the breadth of topics covered and the chronological sequence of the material will prove a useful reference for even the most experienced cybersecurity lawyer and sophisticated organization.

The *Incident Response Guide* is organized into the following sections:

1. Pre-Incident Planning
2. The Incident Response Plan
3. Executing the Incident Response Plan
4. Key Collateral Issues
5. Basic Notification Requirements
6. After-Action Reviews

The appendices of the *Incident Response Guide* include the following items that will be of particular practical benefit to practitioners and organizations:

1. Model Incident Response Plan
2. Model Notification Letters
3. Model Attorney General Breach Notification Letters

The full text of *The Sedona Conference Incident Response Guide* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Incident_Response_Guide.

The Sedona Conference Commentary on Application of Attorney-Client Privilege and Work-Product Protection to Documents and Communications Generated in the Cybersecurity Context

(November 2019)

The Sedona Conference Working Group on Data Security and Privacy Liability (WG11) developed the *Commentary on Application of Attorney-Client Privilege and Work-Product Protection to Documents and Communications Generated in the Cybersecurity Context* ("Commentary") to evaluate the application of the attorney-client privilege and work-product protection doctrine to an organization's cybersecurity information (CI). The Commentary seeks to move the law forward by assessing the arguments for and against the discoverability of CI being determined under general principles of attorney-client privilege and work-product protection law, as opposed to modifying those principles in the context of CI.

The goal of the *Commentary* is to address the absence of "settled law" on this topic by assessing:

1. how the courts have and can be expected to decide, and what organizational practices will be important to a court's decision, regarding whether attorney-client privilege or work-product protection apply to documents and communications generated in the cybersecurity context; and
2. how the development of the law in this area should be informed not just by established attorney-client privilege and work-product protection principles, but also by the policy rationales underlying these principles generally and those that are unique to the cybersecurity context.

The *Commentary* considers various proposals for adapting existing attorney-client privilege and work-product protection law, or developing entirely new protections, in the CI context. To that end, the *Commentary* calls for enacting a qualified—but not absolute—stand-alone cybersecurity privilege under which CI would enjoy some measure of protection against discoverability, regardless of whether lawyers were sufficiently involved in its creation to otherwise qualify for protection. The *Commentary* also calls for state and federal law to recognize a "no waiver" doctrine that provides a data holder's disclosure of CI to law enforcement would not waive any privilege or protection that might otherwise be claimed in future civil litigation.

The full text of *The Sedona Conference Commentary on Application of Attorney-Client Privilege and Work-Product Protection to Documents and Communications Generated in the Cybersecurity Context,* is available free for individual download from The Sedona Conference website at: https://thesedonaconference.org/publication/Commentary_on_Application_of_Attorney-Client_Privilege_and_Work-Product_Protection_to_Documents_and_Communications_Generated_in_the_Cybersecurity_Context.

The Sedona Conference Commentary on Data Privacy and Security Issues in Mergers & Acquisitions Practice (May 2019)

The Sedona Conference Working Group on Data Security and Privacy Liability (WG11) developed the *Commentary on Data Privacy and Security Issues in Mergers & Acquisitions Practice* ("*Commentary*") to provide practical guidance on data privacy and security issues that must be considered in a potential acquisition. In doing so, it approaches these issues from the perspective of the buyer. It is intended to provide a framework for addressing the privacy and security issues that likely will impact a transaction.

The *Commentary* addresses these privacy and security issues in the three basic stages of a transaction:

1. Determining the scope of the acquisition
2. Conducting due diligence
3. Closing and post-closing considerations

At the end of each stage, there is a short summary containing the key "takeaway" points. In addition, the *Commentary* aims to give practical demonstrations of those processes, including sufficient background information to demonstrate how the proposed guidance will work in the real world. Given this approach, the *Commentary* is not intended to be exhaustive and certainly could not be; the scope of the issues that may arise will necessarily turn on the specifics of a given transaction and the terms negotiated by the buyer and the seller.

It is our hope that the Commentary will be of use not only to professionals working on an acquisition, but also to those who will work on the post-deal integration of acquired assets. We have also appended to the *Commentary* a summary of the categories and types of data implicated in the deal analysis (Appendix A); sample representations and warranties that address privacy and security concerns (Appendix B); and basic due-diligence requests (Appendix C).

The Sedona Conference Data Privacy Primer
(January 2018)

The Sedona Conference Working Group on Data Security & Privacy Liability (WG11) developed the *Data Privacy Primer* to provide a practical framework and guide to basic privacy issues in the United States, including identification of key privacy concepts in federal and state laws, regulations, and guidance. The main focus of the *Data Privacy Primer* is on privacy issues arising under civil rather than criminal law. The *Data Privacy Primer* addresses privacy as it exists, and intends to provide background and context for understanding and interpreting current privacy laws and requirements.

The *Data Privacy Primer* is organized into substantive sections of broad privacy categories:

1. Federal and State Governments
2. General Consumer Protection
3. Health
4. Financial
5. Workplace Privacy
6. Student Privacy

Within each of these sections, key U.S. federal and state laws, policies, and considerations from both a compliance and litigation perspective are detailed. Each section also includes a "side bar," which summarizes the key points in each section.

The full text of *The Sedona Conference Data Privacy Primer*, January 2018, is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/The_Sedona_Conference_Data_Privacy_Primer.

The Sedona Conference Commentary on Cross-Border Discovery in U.S. Patent and Trade Secret Cases (July 2023)

The Sedona Conference is pleased to announce publication of the final version of our Commentary on Cross-Border Discovery in U.S. Patent and Trade Secret Cases ("Stage 2")—a joint project of Working Group 10 on Patent Litigation Best Practices and Working Group 12 on Trade Secrets.

The Commentary addresses the significant complexities for courts and counsel in the management of cross-border discovery in light of the growing proliferation of patent and trade secret disputes rising to the level of global litigation. It focuses on best practices in dealing with one particularly vexing aspect of cross-border discovery: the management of applications to U.S. district courts made pursuant to 28 U.S.C. Section 1782 seeking evidence encompassing confidential or trade secret information to be used in a proceeding before a foreign or international tribunal.

The full text of *The Sedona Conference Commentary on Cross-Border Discovery in U.S. Patent and Trade Secret Cases* (July 2023) is available free for individual download from The Sedona Conference website at:
https://thesedonaconference.org/publication/Commentary_on_Cross-Border_Discovery_in_US_Patent_and_Trade_Secret_Cases.

The Sedona Conference Commentary on Cross-Border Privilege Issues (July 2022)

The Sedona Conference Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6) developed the *Commentary on Cross-Border Privilege Issues* ("*Commentary*") to (1) provide an overview of select laws and the differences between them and (2) set forth practice points to consider in managing and resolving the conflicts that can arise in multijurisdictional matters where the protections afforded in one jurisdiction may not be recognized in, or may be in conflict with, those of another.

Section I is the introduction to the *Commentary*. Section II of the *Commentary* broadly explains the distinctions between common law and civil law privilege and other legal protections against disclosure. Section III lays out practical considerations for navigating these differences. Section IV explores the choice-of-law analysis used by some courts for deciding the application of privilege laws. Finally, Section V provides an appendix of privilege and other legal protections in selected exemplar jurisdictions.

The practice points outlined in Section III are as follows:

- **Practice Point 1:** Be Mindful That Approaches to Privilege Differ
- **Practice Point 2:** Be Aware of the Limitations on In-House Counsel Privilege
- **Practice Point 3:** Consider Applicable Governmental and Regulatory Privileges and Weigh the Risks of Waiver before Making a Regulatory Disclosure
- **Practice Point 4:** Be Proactive in Exploring and Exercising Options to Protect Applicable Privileges
- **Practice Point 5:** Assess Possible Privilege Waivers and Take Practical Steps to Minimize Waiver Risks Going Forward
- **Practice Point 6**: Special Planning is Necessary for Parallel Proceedings and Simultaneous or Sequential Litigation
- **Practice Point 7**: Assist Courts with Cross-Border Privilege Issues, as Courts May Lack Familiarity with Relevant Jurisdictional Laws
- **Practice Point 8**: Understand Applicable Choice-of-Law and Comity Principles

The full text of *The Sedona Conference Commentary on Cross-Border Privilege Issues* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Cross-Border_Privilege_Issues.

The Sedona Conference Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders (April 2020)

The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6) developed the *Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders* ("*Commentary*") to:

1. provide a practical guide to corporations and others who must make day-to-day operational decisions regarding the transfer of data across borders; and
2. provide a framework for the analysis of questions regarding the laws applicable to cross-border transfers of personal data; and
3. encourage governments to harmonize their domestic laws to facilitate global commerce.

Basic principles of international law relating to sovereignty, due diligence, jurisdiction, and the rights enjoyed by natural persons can help support a set of principles that can serve as a framework for analyzing cross-border transfers of personal and confidential data in a global economy. This *Commentary* puts forth six principles to guide readers in determining which nation's laws should apply in a given context.

Principle 1: A nation has nonexclusive jurisdiction over, and may apply its privacy and data protection laws to, natural persons and organizations in or doing business in its territory, regardless of whether the processing of the relevant personal data takes place within its territory.

Principle 2: A nation usually has nonexclusive jurisdiction over, and may apply its privacy and data protection laws to, the processing of personal data inextricably linked to its territory.

Principle 3: In commercial transactions in which the contracting parties have comparable bargaining power, the informed choice of the parties to a contract should determine the jurisdiction or applicable law with respect to the processing of personal data in connection with the respective commercial transaction, and such choice should be respected so long as it bears a reasonable nexus to the parties and the transaction.

Principle 4: Outside of commercial transactions, in which the natural person freely makes a choice, a person's choice of jurisdiction or law should not deprive him or her of protections that would otherwise be applicable to his or her data.

Principle 5: Data in transit ("Data in Transit") from one sovereign nation to another should be subject to the jurisdiction and the laws of the sovereign nation from which the data originated, such that, absent extraordinary circumstances, the data should be treated as if it were still located in its place of origin.

Principle 6: Where personal data located within, or otherwise subject to, the jurisdiction or the laws of a sovereign nation is material to a litigation, investigation, or other legal proceeding within another sovereign nation, such data shall be provided when it is subject to appropriate safeguards that regulate the use, dissemination, and disposition of the data.

The full text of *The Sedona Conference Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_and_Principles_on_Jurisdictional_Conflicts_over_Transfers_of_Personal_Data_Across_Borders.

The Sedona Conference International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations (May 2018)

In the summer of 2013, The Sedona Conference's Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6) began a dialogue on developing practical guidelines and principles to help organizations, regulators, courts, and other stakeholders handle government or internal investigations that necessitate the transfer of Protected Data across national borders. That dialogue ultimately resulted in *The Sedona Conference International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices* ("*International Investigations Principles*").

WG6 began the dialogue that led to International Investigations Principles because while it recognized that its International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation & Discovery of Protected Data in U.S. Litigation ("International Litigation Principles") offers helpful guidance to practitioners and courts in reconciling U.S. Litigation discovery obligations with data protection rights, it also recognized that International Litigation Principles is not always helpful, or even applicable, in the context of investigations.

The resulting *International Investigations Principles* provides eight Principles to guide Organizations in planning for and responding to investigations while ensuring that Protected Data is safeguarded at all times against avoidable risks of disclosure.

The eight Principles are:

1. Organizations doing business across international borders, in furtherance of corporate compliance policies, should develop a framework and protocols to identify, locate, process, transfer, or disclose Protected Data across borders in a lawful, efficient, and timely manner in response to Government and Internal Investigations.
2. Data Protection Authorities and other stakeholders should give due regard to an Organization's need to conduct Internal Investigations for the purposes of regulatory compliance and other legitimate interests affecting corporate governance, and to respond adequately to Government Investigations.
3. Courts and Investigating Authorities should give due regard both to the competing legal obligations, and the costs, risks, and burdens confronting an Organization that must retain and produce information relevant to a legitimate Government Investigation, and the privacy and data protection inter-

ests of Data Subjects whose personal data may be implicated in a cross-border investigation.

4. Where the laws and practices of the country conducting an investigation allow it, the Organization should at an early stage of a Government Investigation engage in dialogue with the Investigating Authority concerning the nature and scope of the investigation and any concerns about the need to produce information that is protected by the laws of another nation.

5. Organizations should consider whether and when to consent to exchanges of information among Investigating Authorities of different jurisdictions in parallel investigations to help minimize conflicts among Data Protection Laws.

6. Investigating Authorities should consider whether they can share information about, and coordinate, parallel investigations to expedite their inquiries and avoid, where possible, inconsistent or conflicting results and minimize conflicts with Data Protection Laws.

7. Courts and Data Protection Authorities should give due regard to the interests of a foreign sovereign seeking to investigate potential violations of its domestic laws.

8. A party's conduct in undertaking Internal Investigations and complying with Investigating Authorities' requests or demands should be judged by a court, Investigating Authority, or Data Protection Authority under a standard of good faith and reasonableness.

The full text of *The Sedona Conference International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/International_Investigations_Principles.

The Sedona Conference International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition, 2017)

The rapid proliferation of electronic information and the increasing interdependence amongst individuals, multi-national companies, and governments arising from a global marketplace present novel and unique legal challenges that previously did not exist. Around the world, and particularly in Europe, nations have adopted data protection laws that restrict the collection, processing, retention, and transfer of personal data. The result has been that one of the challenges in the new global economy is the conflict that arises when a party is obligated to disclose information in one forum (e.g., a United States court) but that information is located outside the United States (e.g., typically in the European Union or EU) and is protected by a data protection law, "blocking statute," bank secrecy law, or other regulation which prohibits its disclosure.

In 2011, The Sedona Conference's Working Group on International Electronic Information Management, Discovery, and Disclosure ("Working Group 6"), produced the first edition of the *International Principles on Discovery, Disclosure & Data Protection*, which articulated six Principles with commentary and useful forms to assist courts and litigants in addressing the tension between the U.S. tradition of liberal discovery and emerging data protection laws in other nations. Working Group 6's mandate is an important one: to bring together some of the most experienced attorneys, judges, privacy and compliance officers, technology-thought leaders, and academics from around the globe in a dialogue about the international management, discovery, and disclosure of electronically stored information ("ESI") involved in cross-border disputes. The 2011 *International Principles* was well-received by practitioners, and individual members of the EUs' Article 29 Working Party on data protection considered it to be both a positive contribution and an opening for further dialogue.

In 2016, the EU adopted the General Data Protection Regulation (GDPR), which updates and consolidates the data protection laws of the separate EU Member States. At the same time, the most common mechanism for the lawful transfer of personal data from Europe to the U.S., the "Safe Harbor," was declared invalid by the Court of Justice of the European Union, leading to the negotiation of a new mechanism, "Privacy Shield." The GDPR will go into effect in May of 2018, and practice under the new Privacy Shield is just beginning to develop. To address uncertainty during this transitional period, Working Group 6 has updated the commentary to the Principles and significantly revised the model practice documents. The Principles themselves have not been substantively changed, having withstood the test of turbulent times.

These six Principles are:

1. With regard to data that is subject to preservation, disclosure, or discovery in a U.S. legal proceeding, courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws.

2. Where full compliance with both Data Protection Laws and preservation, disclosure, and discovery obligations presents a conflict, a party's conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness.

3. Preservation, disclosure, and discovery of Protected Data should be limited in scope to that which is relevant and necessary to support any party's claim or defense in order to minimize conflicts of law and impact on the Data Subject.

4. Where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect Protected Data and minimize the conflict.

5. A Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted.

6. Data Controllers should retain Protected Data only as long as necessary to satisfy legal or business needs. While a legal action is pending or remains reasonably anticipated, Data Controllers should preserve relevant information, including relevant Protected Data, with appropriate data safeguards.

In the Transitional Edition, these six Principles are accompanied by detailed commentary and analysis, as well as a Bibliography, a Model U.S. Federal Court Order Addressing Cross-Border ESI Discovery, a Model U.S. Federal Court Protective Order, and a model Cross-Border Data Safeguarding Process + Transfer Protocol.

The full text of *The Sedona Conference International Principles on Discovery,Disclosure & Data Protection in Civil Litigation (Transitional Edition)* is available free
for individual download from The Sedona Conference website at
https://thesedonaconference.org/publication/International_Litigation_Principles.

The Sedona Conference Practical In-House Approaches for Cross-Border Discovery & Data Protection (June 2016)

Building on the groundbreaking *International Principles on Discovery, Disclosure and Data Protection*, *The Sedona Conference Practical In-House Approaches for Cross-Border Discovery and Data Protection* aims to provide the practical guidance that organizations and in-house counsel need to navigate challenging cross-border data transfer and discovery issues, and effectively implement the International Principles. This publication represents the collective effort of members of Sedona Working Group 6 on International Electronic Information Management, Discovery and Disclosure, with input from the public on its recommendations.

The commentary section of the publication is organized around eight essential Practice Points:

1. Balance the need for urgency in preserving information with the need to proceed deliberately in countries with comprehensive Data Protection Laws.
2. As early as possible, meet and reach agreements with key stakeholders on a plan that sets expectations regarding legal obligations, roles and responsibilities, and a reasonable timeline.
3. Identify and define privacy issues with opposing parties or regulators through Outside counsel where possible.
4. Set up transparency "checkpoints," beginning with preservation and continuing through the life of the matter, to avoid revocation of consent.
5. Plan a successful in-country collection with detailed surveys of appropriate systems well in advance, and by soliciting support from key stakeholders, bothin corporate departments and local business units.
6. Use the processing stage of discovery as an opportunity to balance compliance with both discovery and Data Protection Laws, thereby demonstrating due respect for Data Subjects' privacy rights.
7. During review of data for production and disclosure, parties may consider ways to limit the production of Protected Data; when production of Protected Data is necessary, safeguards can be established to demonstrate due respect for both discovery and Data Protection Laws.
8. To avoid keeping data longer than necessary, counsel should prepare to release legal holds and return or dispose of data promptly upon termination of a matter.

The publication goes beyond commentary on the issues by providing a "tool kit" for implementing an effective in-house data protection and cross-border discovery process that includes a detailed model corporate policy, a model cross-border discovery management checklist, model Frequently Asked Questions language and a useful infographic for employee and client education, and an exemplar "heat map" for identifying cross-border data protection issues most relevant to a particular enterprise or project.

The full text of *The Sedona Conference Practical In-House Approaches for Cross-Border Discovery & Data Protection* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Practical_In-House_Approaches_for_Cross-Border_Discovery_and_Data_Protection.

The Sedona Conference Commentary on Monetary Remedies in Trade Secret Litigation (July 2023)

The available remedies for trade secret misappropriation drive and define litigation on these claims. Recognizing this, The Sedona Conference created drafting teams of its members to identify, organize, and present consensus, nonpartisan principles on available remedies for trade secret misappropriation, which include both non-monetary and monetary remedies. The previously published *Commentary on Equitable Remedies in Trade Secret Litigation* provides principles for nonmonetary remedies. This *Commentary* provides them for monetary remedies.

The rules for what money a successful trade secret claimant can recover are easy to state but often difficult to apply. This *Commentary* seeks to be a resource to assist parties and decisionmakers in addressing monetary remedies and suggests effective methods for determining whether, and in what amount, to award monetary relief for trade secret misappropriation.

To achieve these aims, this *Commentary* focuses on the statutory and decisional law that provides for the three core types of damages in trade secret cases: actual loss, unjust enrichment, and, in many cases, royalties. This *Commentary* also analyzes the difficult issues that must be grappled with regarding such damages, including apportionment, causation, reasonable certainty, the applicability and inapplicability of patent damages law precedent in trade secret cases, and many more.

This *Commentary* presents three Principles for the governance and management of trade secrets:

Principle 1 Monetary remedies should fairly compensate the trade secret owner for damages sustained as a result of misappropriation.

Principle 2 The existence of damages and the measurement of a monetary damages award for misappropriation must not be speculative, but the amount of damages need not be proved with mathematical certainty.

Principle 3 Multiple theories of measuring damages for misappropriation may be applied so long as there is no double counting.

The full text of *The Sedona Conference Commentary on Monetary Remedies in Trade Secret Litigation* is available free for individual download from The Sedona Conference website at: https://thesedonaconference.org/publication/Commentary_on_Monetary_Remedies_in_Trade_Secret_Litigation.

The Sedona Conference Commentary on the Governance and Management of Trade Secrets (July 2023)

This Commentary was written from both legal and business perspectives as a useful reference for the design and implementation of trade secret governance and protection programs in corporate environments. It can also provide insight to litigators and judges about the practical ways companies approach the "reasonable efforts" requirement in trade secret law. The central message is that programs to manage trade secrets, like other business processes, should align with business objectives in the context of the needs of the specific business. Ideally, trade secret management should be contextual and strategic, and not just a collection of "boilerplate" forms and protocols that may bear little relationship to the actual trade secrets and risk environment of a particular company.

While trade secret management demands strategic business thinking, it also has a legal dimension. The existence of a trade secret depends in part on whether the company has exercised "reasonable efforts" (or "reasonable measures") directed at maintaining its secrecy. This standard corresponds to the relevant circumstances of each enterprise, so that there can be no "one size fits all." In effect it suggests that the judge or jury apply the same kind of analysis; namely, an assessment of the value of, and risks to, specific trade secrets in the context of the company's particular business and resources. We hope that this paper will help management formulate a proactive, tailored, and practical approach to managing trade secret assets that will address both business and legal requirements.

This *Commentary* presents four Principles for the governance and management of trade secrets:

Principle 1 Trade secrets should be protected by efforts that are reasonable under the circumstances to maintain their secrecy and value. Absolute secrecy is neither possible nor required. There is no one-size-fits-all approach.

Principle 2 A trade secret protection program should be actionable and achievable, rather than conceptual or aspirational. Once implemented, it should be periodically evaluated and adjusted as the company's trade secrets, business, and risk environment evolve.

Principle 3 A trade secret protection program should align with business goals and measurable objectives such as (1) securing and maintaining competitive advantage for the business; (2) leveraging trade secrets to commercialize new products and services; (3) supporting, generating, and incentivizing continued innovation; (4) extracting additional value from trade secrets through licensing, acquisitions, or secured financing; and (5) enforcing trade secret rights as necessary.

Principle 4 Trade secret governance generally requires an integrated enterprise approach that should accommodate and satisfy multiple and potentially conflicting corporate interests, including effective controls, information governance and data security, talent acquisition and retention, operational efficiency, disciplined budgets, reasonable return on investment, third-party information sharing demands, and legal enforceability.

The full text of *The Sedona Conference Commentary on the Governance and Management of Trade Secrets* is available free for individual download from The Sedona Conference website at: https://thesedonaconference.org/publication/Commentary_on_Governance_and_Management_of_Trade_Secrets.

The Sedona Conference Framework for Analysis on Trade Secret Issues Across International Borders: Extraterritorial Reach

(June 2022)

The *Framework for Analysis on Trade Secret Issues Across International Borders: Extraterritorial Reach* addresses the extraterritorial reach of United States federal and state trade secret law. Trade secret misappropriation is increasingly a cross-border problem, with conduct that is difficult to reach in the United States. In some instances, foreign parties are accused of misappropriating U.S. trade secrets but never enter the United States physically and have little or no presence in the United States. Other cases involve parties and incidents that span multiple countries, including the United States. It often is equally difficult to address overseas and extraterritorial misappropriation through foreign legal proceedings due to shortcomings in national laws and enforcement in many countries. Moreover, it may be the case that no one country's courts are able to offer a complete remedy.

Finding a remedy for such cross-border claims in U.S. courts poses several challenges, particularly territoriality, which limits the ability of a country's courts to apply its laws to conduct outside its borders. Under U.S. law, territoriality gives rise to a presumption against extraterritorial application of law. Nevertheless, the presumption against extraterritoriality is just that—a presumption. There are exceptions to the rule. For instance, the presumption against extraterritorial application of domestic law does not entirely preclude the use of domestic laws and forums to seek relief for extraterritorial acts.

This *Framework* thus identifies key means by which U.S. trade secret law reaches conduct abroad. For each of these means, it identifies primary areas of agreement, disagreement, and ambiguity. It catalogs some successful approaches, offers guidance as to how they can be used, and identifies potential limitations of existing approaches.

The discussion here is framed as a resource to parties and lawyers seeking to remedy a misappropriation of trade secrets where some or all of the conduct, parties, or evidence are outside of the United States. Nevertheless, this *Framework* should serve equally as a resource to a party defending a claim for misappropriation of trade secrets with extraterritorial aspects—the framing will serve to ensure comprehensive coverage.

The first part of the *Framework* identifies six key means of reaching conduct abroad:

- claims pursuant to the Defend Trade Secrets Act
- claims pursuant to state trade secret laws
- the International Trade Commission

- criminal prosecution
- extrajudicial regulatory remedies against foreign wrongdoers
- litigation abroad

The second part of the *Framework* then addresses significant challenges when parties attempt to use these means to reach conduct abroad:

- sovereign immunities
- choice of law issues
- jurisdiction and venue
- where and how to get evidence
- enforceability of trade secret judgments against foreign entities

The full text of *The Sedona Conference Framework for Analysis on Trade Secret Issues Across International Borders: Extraterritorial Reach*, June 2022 edition, is available free for individual download from The Sedona Conference website at: https://thesedonaconference.org/publication/Trade_Secret_Issues_Across_International_Borders_Extraterritorial_Reach.

The Sedona Conference Commentary on Protecting Trade Secrets in Litigation About Them (March 2022)

Trade secrets are a property interest that can be destroyed by disclosure. This makes litigation of trade secrets unique; by bringing claims seeking to remedy misappropriation, a trade secret owner puts these secret information assets at issue in the public litigation process. Without the ability to protect the secrecy of trade secrets in litigation, the law of trade secrets would disappear, as it would be impossible to enforce trade secret rights in the face of misappropriation. Both the Uniform Trade Secrets Act and the Defend Trade Secrets Act explicitly acknowledge the need to protect trade secrets in litigation.

But this issue of protection runs into competing policy objectives: First, defendants need information about the claims to mount an effective defense, and second, the public generally has a constitutional right to access judicial proceedings. In this *Commentary on Protecting Trade Secrets in Litigation About Them*, Working Group 12 attempts to reconcile these important objectives with the need to protect trade secrets when litigating misappropriation claims. This *Commentary* offers consensus recommendations to parties and courts for addressing these thorny issues in various contexts, including access to trade secret information by in-house counsel, experts, employees, and attorneys who prosecute patents, as well as providing consensus guidance to parties and courts about balancing the right to public access with the trade secret owner's right to maintain the secrecy of its trade secrets.

This *Commentary* also addresses logistical issues that often arise in trade secret cases. In virtually all such cases, discovery is governed by a protective order. This working group provides guidance around how these orders should be drafted and how parties should exchange information pursuant to a protective order. The goal is to avoid unnecessary overdesignation, which burdens parties and the court, while allowing for efficient exchange of information.

This *Commentary* presents six Principles for protecting trade secrets in litigation about them:

Principle 1 Whether a party's in-house attorneys, experts, or employees should be permitted to have access to the trade secrets of another party should be determined by balancing the risk of disclosure and harm to the producing party with the need for the other party to have the information in order to properly prepare its case.

Principle 2 In civil proceedings, the public has a qualified right of access to documents filed with a court that are relevant to adjudicating the merits of a controversy. In compelling circumstances, a court may exercise its discretion to deny public access to submitted documents to protect the privacy, confidentiality or other rights of the litigants.

Principle 3 Because public disclosure of a trade secret in litigation could destroy its value, if the trade secret owner establishes that certain information reveals all or a meaningful part of a trade secret, such information should be restricted from public disclosure, in both filings and open court. Restrictions should be as narrowly tailored as necessary to protect the trade secrets at issue.

Principle 4 In cases to be tried before a jury, restrictions on disclosure of a trade secret at trial should be implemented in a manner that minimizes any prejudicial effects of the restrictions.

Principle 5 A court does not need to make a conclusive determination as to whether a party's information qualifies as a trade secret before ordering appropriate protections. Instead, the court should determine whether that party has credibly identified the existence of a trade secret, making a particularized finding regarding the specific information that is subject to protection.

Principle 6 The parties should cooperate in good faith to develop and implement a protective order that balances: (a) the need to protect trade secret information; (b) the right of both parties to receive timely disclosures and discovery responses; and (c) the right to have specified nonattorney representatives also timely review the other party's discovery responses.

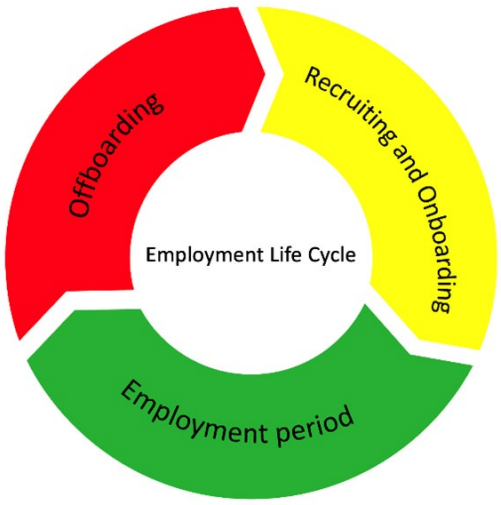
The full text of *The Sedona Conference Commentary on Protecting Trade Secrets in Litigation About Them* is available free for individual download from The Sedona Conference website at: https://thesedonaconference.org/publication/Commentary_on_Protecting_Trade_Secrets_in_Litigation_About_Them.

The Sedona Conference Commentary on Protecting Trade Secrets Throughout The Employment Life Cycle
(March 2022)

Employees are at the center of most aspects of trade secrets: Trade secrets cannot exist without the work of employees, cannot be protected without the efforts of employees, and would rarely be compromised or lost without the conduct of employees. This *Commentary on Protecting Trade Secrets throughout the Employment Life Cycle* focuses on the inherent potential tensions this creates in the employer-employee relationship.

While in most circumstances, employers and employees will be aligned in protecting trade secrets for their mutual benefit at the beginning and during the employment relationship, at the end of the relationship, there is an inherent tension between an employer's interest in protecting its trade secrets and an employee's interest in engaging in future employment. This tension is further complicated by the fact that, although the departing employee is at the end of one employment life cycle, they are typically simultaneously at the beginning of the next, where the former's employer's risk of loss of its trade secrets corresponds directly to the new employer's risk of infiltration of those same trade secrets.

This *Commentary* addresses these issues through a chronological view of the employment relationship, from recruiting and onboarding, to the period of employment, to offboarding, and back to onboarding, as follows:



This *Commentary* presents four Principles for protecting trade secrets in litigation about them:

Principle 1 There is an inherent tension between an employer's interest in protecting its trade secrets and an employee's interest in engaging in future employment. Employers should tailor their policies and procedures to guard against the risk of unlawful use or disclosure of their trade secrets, while avoiding inappropriately restricting their former employees' application of their general knowledge, skill, and experience in their next employment.

Principle 2 Employers should provide timely and sufficient notice of what they claim as their trade secrets, the policies and procedures to be followed by employees to protect those trade secrets, and any restrictions the employers intend to impose on the future mobility of their prospective and current employees.

Principle 3 Employees and new employers should take into account the legitimate interests of former employers in their trade secrets, and employees and new employers should take reasonable steps to mitigate against the risks of misappropriation of the former employers' trade secrets.

Principle 4 In response to an impending employee departure, the employer should identify, address, and communicate as appropriate legitimate concerns about the departing employee's compliance with their continuing obligation to protect the employers' trade secrets.

The full text of *The Sedona Conference Commentary on Protecting Trade Secrets throughout the Employment Life Cycle* (March 2022) is available free for individual download from The Sedona Conference website at:
https://thesedonaconference.org/publication/Commentary_on_Protecting_Trade_Secrets_Throughout_Employment_Life_Cycle.

The Sedona Conference Commentary on Equitable Remedies in Trade Secret Litigation (March 2022)

Obtaining or resisting some form of equitable relief is a key component of many trade secret disputes, both at an early stage and following trial on the merits. The *Commentary on Equitable Remedies in Trade Secret Litigation* is designed to be a resource to assist parties and decision-makers in conducting this analysis. The *Commentary* reminds readers that equitable relief in trade secret disputes does not stand apart from general principles of equity and explores how those principles have been applied to trade secret disputes. Given the nature of equitable relief, the *Commentary* does not, and by definition, could not, urge a one-size-fits-all approach to equitable relief in trade secret disputes. Rather, it focuses on exploring the key factors courts consider in assessing any equitable relief and considers how courts have applied these basic equitable factors to evaluating and fashioning equitable relief in trade secret disputes.

Trade secret disputes often arise on an emergency basis before either party has developed a full evidentiary record. The perceived "need for speed" can lead to a number of problems that the *Commentary* works to address. First, it offers suggestions for assessing how an early remedy can be calibrated to the availability of evidence and whether targeted expedited discovery may assist the parties and the court in evaluating early requests. Second, it emphasizes that equitable relief, or its denial, must always be tied to the direct and circumstantial evidence presented to the court and the reasonable inferences therefrom and not rely simply on oft-cited mantras or invocations of presumptions. It offers examples of how such assessments have been made in a variety of cases in jurisdictions across the country. Finally, the *Commentary* gives guidance for selecting, scoping, and drafting a variety of equitable remedies to suit the needs of a variety of disputes.

This *Commentary* presents five Principles for equitable remedies in trade secret litigation:

Principle 1 What constitutes an appropriate equitable remedy may change over the course of the dispute given the evidence available to the parties and the reasonable inferences to be drawn therefrom.

Principle 2 On all motions for interim equitable relief, the court should consider the nature and urgency of the harm alleged and the extent to which material facts are undisputed, are known or accessible to either or both parties, or require further discovery to resolve.

Principle 3 On motions for preliminary equitable relief, the parties and the court should consider whether targeted expedited discovery is appropriate.

Principle 4 The parties and the courts should evaluate the available evidence and the parties' respective burdens before determining whether any presumptions should apply to requests for equitable relief.

Principle 5 The court may incorporate provisions into orders granting equitable relief designed to balance the hardships between the parties.

The full text of *The Sedona Conference Commentary on Equitable Remedies in Trade Secret Litigation* is available free for individual download from The Sedona Conference website at: https://thesedonaconference.org/publication/Commentary_on_Equitable_Remedies_in_Trade_Secret_Litigation.

The Sedona Conference Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases (October 2020)

The Sedona Conference Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases provides Principles and Guideline recommendations for Trade Secrets litigation.

A fundamental question in every case involving a claim of trade secret misappropriation is: what are the alleged trade secrets that are the subject of the claim? This question sets apart trade secret law from other major categories of intellectual property (patents and copyrights) in which the alleged intellectual property is defined and registered with a regulatory body before litigation begins.

The burden is on the party asserting trade secret misappropriation to answer this question by "identifying" the alleged trade secrets. While this requirement for "identification" is ubiquitous, the rules for doing so are not clear or consistent.

The Sedona Conference's Working Group 12 (WG12) resolved that its first commentary on trade secret law would address the identification question. This *Commentary* represents WG12's views about certain aspects of identification, including when an identification must be provided, what an identification must contain, and how an identification can be amended.

This *Commentary* presents four practical Principles for the Proper Identification of Asserted Trade Secrets in Misappropriation Cases:

Principle 1 The identification of an asserted trade secret during a lawsuit is not an adjudication of the merits and is not a substitute for discovery

Principle 2 The party claiming misappropriation of a trade secret should identify in writing the asserted trade secret at an early stage of the case.

Principle 3 The party claiming the existence of a trade secret must identify the asserted trade secret at a level of particularity that is reasonable under the circumstances.

Principle 4 The identification of an asserted trade secret may be amended as the case proceeds.

The full text of *The Sedona Conference Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Proper_Identification_of_Trade_Secrets_in_Misappropriation_Cases.

The Sedona Conference Commentary on Patent Litigation Best Practices: Streamlining Lower-Value Patent Cases (July 2023)

The Sedona Conference is pleased to announce publication of the final version of its *Commentary on Patent Litigation Best Practices: Streamlining Lower-Value Patent Cases Chapter*, a project of Working Group 10 on Patent Litigation Best Practices (WG10).

In preparing its *Commentary on Patent Litigation Best Practices: Streamlining Lower-Value Patent Cases Chapter (Commentary)*, WG10 ascertained that in the patent cases that went to trial between 2019 and 2021 where the patentee was successful in showing that at least one claim was infringed and not invalid, the amount of damages awarded was under $15 million 74 percent of the time. The rules and procedures that govern patent cases in the U.S. district courts, however, generally do not distinguish between patent cases where hundreds of millions of dollars are at stake and those where the amount at issue is a fraction of that amount.

As a result, parties to a "lower value" patent case often expend disproportionate amounts of time and money litigating the case. The consensus of WG10 is that patent litigants and courts would benefit from a formalized, streamlined program for resolving lower-value patent cases. It is contemplated that the program, when used, will significantly reduce both the time and cost associated with resolving patent cases where the amount at issue is in the range of $10 million or less. Thousands of patent cases every year could be eligible for and benefit from the program.

The *Commentary* describes the program's features, including required bench trials, optional participation by the parties, significant reductions in discovery, asserted claims, prior art, and defenses, and an early claim construction hearing.

The full text of *The Sedona Conference Commentary on Patent Litigation Best Practices: Streamlining Lower-Value Patent Cases Chapter* is available free for individual download from The Sedona Conference website at:
https://thesedonaconference.org/publication/Streamlining_Lower-Value_Patent_Cases.

The Sedona Conference Framework for Analysis for the Efficient Resolution of Disputes before the Forthcoming European Unified Patent Court (May 2023)

The Sedona Conference and Working Group 10 on Patent Litigation Best Practices are pleased to announce publication of the final version of our *Framework for Analysis for the Efficient Resolution of Disputes before the Forthcoming European Unified Patent Court*.

The publication provides guidance for all stakeholders—patentees, defendants, practitioners, and judges—who may find themselves involved in proceedings before the European Union's Unified Patent Court (UPC) system, a new patent jurisdiction whose rulings will potentially span all of the European Union. The UPC, beginning operations in June 2023, offers the potential for more cost-efficient litigation, but it arrives with significant uncertainty as to how the court will manage its proceedings. To mitigate these uncertainties, judges and practitioners need consider not only a whole new set of provisions and rules, but also the existing case law under current European patent regimes in order to determine how to best resolve disputes in an efficient, fair, and equitable manner.

The full text of *The Sedona Conference Framework for Analysis for the Efficient Resolution of Disputes before the Forthcoming European Unified Patent Court*, May 2023 Final Version, is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Framework_for_Analysis_for_Resolution_of_Disputes_before_European_Unified_Patent_Court

The Sedona Conference Framework for Analysis of Standard-Essential Patent (SEP) and Fair, Reasonable, and Non-Discriminatory (FRAND) Licensing and Royalty Issues (Jan. 2023 edition)

The Sedona Conference and Working Group 9 on Patent Damages and Remedies are pleased to announce publication of the final, post-public-comment edition of our Framework for Analysis of Standard-Essential Patent (SEP) and Fair, Reasonable, and Non-Discriminatory (FRAND) Licensing and Royalty Issues ("US Edition").

The publication is designed to help practitioners and the judiciary identify and put into the appropriate context the types of issues that frequently arise in infringement suits relating to standard-essential patents (SEPs) and commitments to license patents on fair, reasonable, and non-discriminatory (FRAND) terms.

The full text of *The Sedona Conference Framework for Analysis of Standard-Essential Patent (SEP) and Fair, Reasonable, and Non-Discriminatory (FRAND) Licensing and Royalty Issues*, is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Framework_for_Analysis_of_SEP_and_FRAND_Licensing_and_Royalty_Issues.

The Sedona Conference Executive Summary: Working Group 10 on Patent Litigation Best Practices & Working Group 9 on Patent Damages and Remedies

The Sedona Conference's Working Group 10 on Patent Litigation Best Practices (WG10) and Working Group 9 on Patent Damages and Remedies (WG9) have published numerous consensus, nonpartisan documents in recent years, collectively designed to move the law and practice of patent litigation forward in a reasoned and just way, consisting of:

I. *WG10 Commentary on Patent Litigation Best Practices*
   A. *Introductory Chapter* (July 2015 Edition)
   B. *Case Management Issues from the Judicial Perspective Chapter* (Dec. 2015 Edition)
      1. *Section on Exceptional Case Determinations* (Oct. 2016 public comment version)
   C. *Pleading Standards Under* Iqbal/Twombly *Chapter* (Oct. 2017 Edition)
   D. *Mediation Chapter* (Apr. 2017 Edition)
   E. *Parallel USPTO Proceedings Chapter ("Stage One")* (Oct. 2016 Edition)
   F. *Parallel USPTO Proceedings Chapter ("Stage Two")* (July 2017 public comment version)
   G. *Discovery Chapter* (Dec. 2015 Edition)
   H. *Summary Judgment Chapter* (Oct. 2015 Edition)
   I. *Section 101 Motions on Patentable Subject Matter Chapter* (Sept. 2016 public comment version)
   J. *Use of Experts,* Daubert*, and Motions* in Limine *Chapter* (Dec. 2015 Edition)
   K. *Willful Infringement Chapter* (July 2020 public comment version)
   L. *Chapter on Streamlining Lower-Value Patent Cases* (Sept. 2022 public comment version)
   M. *Chapter on International Trade Commission Section 337 Investigations* (May 2019 Edition)
   N. *Biopharma Litigation Chapter* (Oct. 2021 public comment version)
   O. *Framework for Analysis of Venue Selection for Global Patent Litigation: Strategic Considerations* (Oct. 2022 public comment version)
   P. *Framework for Analysis for the Efficient Resolution of Disputes before the Forthcoming European Unified Patent Court* (Jan. 2023 public comment version)
   Q. Commentary on Cross-Border Discovery in U.S. Patent and Trade Secret Cases
      1. *"Stage One"* (May 2021 public comment version)
      2. *"Stage Two"* (Jan. 2023 public comment version)

II. *WG9 Commentaries on Patent Damages and Remedies Commentaries*
   A. *Commentary on Patent Reasonable Royalty Determinations* (Dec. 2016 Edition)
   B. *Commentary on Case Management of Patent Damages and Remedies Issues*

1. *Proposed Model Local Rule for Damages Contentions* (June 2017 Edition)
2. *Patent Damages Hearings* (May 2017 public comment version)

C. *Framework for Analysis of Standard-Essential Patent (SEP) and Fair, Reasonable, and Non-Discriminatory (FRAND) Licensing and Royalty Issues (Stage Two)* (Jan. 2023 Edition)

The complete *Executive Summary: Patent Litigation Best Practices and Patent Damages and Remedies Commentaries*, which includes links to each of the individual publications, is available for download from The Sedona Conference website at:
https://thesedonaconference.org/patent_law_executive_summary.

The Sedona Conference Cooperation Proclamation (July 2008)

The Sedona Conference launches a coordinated effort to promote cooperation by all parties to the discovery process to achieve the goal of a "just, speedy, and inexpensive determination of every action."

The costs associated with adversarial conduct in pre-trial discovery have become a serious burden to the American judicial system. This burden rises significantly in discovery of electronically stored information ("ESI"). In addition to rising monetary costs, courts have seen escalating motion practice, overreaching, obstruction, and extensive, but unproductive discovery disputes – in some cases precluding adjudication on the merits altogether—when parties treat the discovery process in an adversarial manner. Neither law nor logic compels these outcomes.

With this Proclamation, The Sedona Conference launches a national drive to promote open and forthright information sharing, dialogue (internal and external), training, and the development of practical tools to facilitate cooperative, collaborative, transparent discovery. This Proclamation challenges the bar to achieve these goals and refocus litigation toward the substantive resolution of legal disputes.

Cooperation in Discovery is Consistent with Zealous Advocacy

Lawyers have twin duties of loyalty: While they are retained to be zealous advocates for their clients, they bear a professional obligation to conduct discovery in a diligent and candid manner. Their combined duty is to strive in the best interests of their clients to achieve the best results at a reasonable cost, with integrity and candor as officers of the court. Cooperation does not conflict with the advancement of their clients' interests—it enhances it. Only when lawyers confuse advocacy with adversarial conduct are these twin duties in conflict.

Lawyers preparing cases for trial need to focus on the full cost of their efforts – temporal, monetary, and human. Indeed, all stakeholders in the system—judges, lawyers, clients, and the general public—have an interest in establishing a culture of cooperation in the discovery process. Over-contentious discovery is a cost that has outstripped any advantage in the face of ESI and the data deluge. It is not in anyone's interest to waste resources on unnecessary disputes, and the legal system is strained by "gamesmanship" or "hiding the ball," to no practical effect.

Effort to change the culture of discovery from adversarial conduct to cooperation is not utopian.[1] It is, instead, an exercise in economy and logic. Establishing a culture of cooperation will channel

1. Gartner RAS Core Research Note G00148170, *Cost of eDiscovery Threatens to Skew Justice System*, 1D# G00148170, (April 20, 2007) (While noting that "several . . . disagreed with the suggestion [to collaborate in the discovery process] . . . calling it 'utopian'", one of the "take-away's" from the program identified in the

valuable advocacy skills toward interpreting the facts and arguing the appropriate application of law.

Cooperative Discovery is Required by the Rules of Civil Procedure

When the first uniform civil procedure rules allowing discovery were adopted in the late 1930s, "discovery" was understood as an essentially cooperative, rule-based, party-driven process, designed to exchange relevant information. The goal was to avoid gamesmanship and surprise at trial. Over time, discovery has evolved into a complicated, lengthy procedure requiring tremendous expenditures of client funds, along with legal and judicial resources. These costs often overshadow efforts to resolve the matter itself. The 2006 amendments to the Federal Rules specifically focused on discovery of "electronically stored information" and emphasized early communication and cooperation in an effort to streamline information exchange, and avoid costly unproductive disputes.

Discovery rules frequently compel parties to meet and confer regarding data preservation, form of production, and assertions of privilege. Beyond this, parties wishing to litigate discovery disputes must certify their efforts to resolve their difficulties in good faith.

Courts see these rules as a mandate for counsel to act cooperatively.[2] Methods to accomplish this cooperation may include:

1. Utilizing internal ESI discovery "point persons" to assist counsel in preparing requests and responses;
2. Exchanging information on relevant data sources, including those not being searched, or scheduling early disclosures on the topic of Electronically Stored Information;
3. Jointly developing automated search and retrieval methodologies to cull relevant information;
4. Promoting early identification of form or forms of production;
5. Developing case-long discovery budgets based on proportionality principles; and

---

Gartner Report was to "[s]trive for a collaborative environment when it comes to eDiscovery, seeking to cooperate with adversaries as effectively as possible to share the value and reduce costs.").

2. *See*, e.g., *Board of Regents of University of Nebraska v BASF Corp.* No. 4:04-CV-3356, 2007 WL 3342423, at *5 (D. Neb. Nov. 5, 2007) ("The overriding theme of recent amendments to the discovery rules has been open and forthright sharing of information by all parties to a case with the aim of expediting case progress, minimizing burden and expense, and removing contentiousness as much as practicable. [citations omitted]. If counsel fail in this responsibility—willfully or not—these principles of an open discovery process are undermined, coextensively inhibiting the courts' ability to objectively resolve their clients' disputes and the credibility of its resolution.").

6. Considering court-appointed experts, volunteer mediators, or formal ADR programs to resolve discovery disputes.

The Road to Cooperation

It is unrealistic to expect a *sua sponte* outbreak of pre-trial discovery cooperation. Lawyers frequently treat discovery conferences as perfunctory obligations. They may fail to recognize or act on opportunities to make discovery easier, less costly, and more productive. New lawyers may not yet have developed cooperative advocacy skills, and senior lawyers may cling to a long-held "hide the ball" mentality. Lawyers who recognize the value of resources such as ADR and special masters may nevertheless overlook their application to discovery. And, there remain obstreperous counsel with no interest in cooperation, leaving even the best-intentioned to wonder if "playing fair" is worth it.

This "Cooperation Proclamation" calls for a paradigm shift for the discovery process; success will not be instant. The Sedona Conference views this as a three-part process to be undertaken by The Sedona Conference Working Group on Electronic Document Retention and Production (WG1):

> Part I: Awareness—Promoting awareness of the need and advantages of cooperation, coupled with a call to action. This process has been initiated by The Sedona Conference Cooperation Proclamation.
>
> Part II: Commitment—Developing a detailed understanding and full articulation of the issues and changes needed to obtain cooperative fact-finding. This will take the form of a "Case for Cooperation" which will reflect viewpoints of all legal system stakeholders. It will incorporate disciplines outside the law, aiming to understand the separate and sometimes conflicting interests and motivations of judges, mediators and arbitrators, plaintiff and defense counsel, individual and corporate clients, technical consultants and litigation support providers, and the public at large.
>
> Part III: Tools—Developing and distributing practical "toolkits" to train and support lawyers, judges, other professionals, and students in techniques of discovery cooperation, collaboration, and transparency. Components will include training programs tailored to each stakeholder; a clearinghouse of practical resources, including form agreements, case management orders, discovery protocols, etc.; court-annexed e-discovery ADR with qualified counselors and mediators, available to assist parties of limited means; guides for judges faced with motions for sanctions; law school programs to train students in the technical, legal, and cooperative aspects of e-discovery; and programs to assist individuals and businesses with basic e-record management, in an effort to avoid discovery problems altogether.

Conclusion

It is time to build upon modern Rules amendments, state and federal, which address e-discovery. Using this springboard, the legal profession can engage in a comprehensive effort to promote pre-trial discovery cooperation. Our "officer of the court" duties demand no less. This project is not utopian; rather, it is a tailored effort to effectuate the mandate of court rules calling for a "just, speedy, and inexpensive determination of every action" and the fundamental ethical principles governing our profession.