Selected Recent Sedona Conference® Working Group Series™ Publications

(January 2021)

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 web site username and password will speed up the download pro-cess, 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 "down-load 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, alt-hough donations are gratefully accepted. Generally, a qualified member of the drafting or edi-torial 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 Conference Commentary on Legal Holds, Second Edition: The Trigger & The Process (June 2019)
- The Sedona Conference Commentary on Proportionality in Electronic Discovery (May 2017)
- The Sedona Conference Cooperation Proclamation: Resources for the Judiciary, Third Edition (June 2020)

- 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 Primer on Social Media, Second Edition (February 2019)
- The Sedona Conference Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations (May 2018)
- The Sedona Conference Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control" (August 2016)
- The Sedona Conference Federal Rule of Civil Procedure 34(b)(2) Primer: Practice Pointers for Responding to Discovery Requests (March 2018)
- The Sedona Conference TAR Case Law Primer (January 2017)
- The Sedona Conference Guidance for the Selection of Electronic Discovery Providers (April 2017)

Information Governance

- The Sedona Conference Glossary, 5th Edition (February 2020)
- The Sedona Conference Commentary on Information Governance, Second Edition (April 2019)
- The Sedona Conference Commentary on Defensible Disposition (April 2019)

Data Privacy and Cybersecurity

- The Sedona Conference Commentary on Law Firm Data Security (July 2020)
- The Sedona Conference Incident Response Guide (January 2020)
- The Sedona Conference Data Privacy Primer (January 2018)
- 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 Commentary on the Enforceability in U.S. Courts of Orders and Judgments Entered under GDPR (January 2021)
- The Sedona Conference Commentary on a Reasonable Security Test, Public Comment Version (September 2020)

Cross-Border Data Transfers

- The Sedona Conference International Litigation Principles on Discovery, Disclosure & Data Protection in Civil Litigation, Transitional Edition (January 2017)
- The Sedona Conference International Investigations Principles (May 2018)
- The Sedona Conference Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders (April 2020)

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

Trade Secrets

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

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.

© 2017 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

The Sedona Conference Commentary on Legal Holds, Second Edition: (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.

©2019 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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

© 2017 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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.

©2020 The Sedona Conference.
Reprinted courtesy of The Sedona Conference.

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.

©2020 The Sedona Conference.
Reprinted courtesy of The Sedona Conference.

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

©2019 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

The Sedona Conference Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control" (July 2016)

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 full text of *The Sedona Conference Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Commentary_on_Rule_34_and_ Rule_45_Possession_Custody_or_Control.

© 2016 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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.

©2018 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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.

©2018 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

The Sedona Conference TAR Case Law Primer
(January 2017)

In just a few short years, the use of technology-assisted review (TAR) for the exploration and classification of large document collections in civil litigation has evolved from a theoretical possibility to an essential tool in the litigator's toolbox. However, its widespread application— and the realization of its potential benefits—has been impeded by uncertainty about its acceptance by the courts as a legitimate alternative to costly, time-consuming manual review of documents in discovery. This *Primer* analyzes decisions from more than 30 state, federal, and foreign courts and administrative agencies that have been required to opine on the efficacy of TAR in a variety of circumstances, and explores the evolution in the courts' thinking.

The *Primer* is the product of more than a year of development and dialogue within The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It was originally conceived as a chapter of a larger Commentary on the use of TAR in civil litigation, but the rapid development of the case law, the volume of court decisions, and the importance of those decisions in shaping legal practice in real time required that an exposition of the case law be made available on a faster timetable than WG1's usual dialogue and consensus-building process allowed. For that reason, the *Primer* strives to present the case law in as neutral a fashion as possible. It avoids making any recommendations regarding particular TAR methodologies, nor does it propose any principles, guidelines, or best practices for TAR application, independent of those suggested by the courts themselves.

As the title suggests, the *Primer* is a starting point. The evolution in the case law is far from complete, nor is the analysis. We welcome your input on the *Primer* as we continue to receive new decisions that present novel facts, issues, and arguments. Your comments and suggestions may be sent to comments@sedonaconference.org.

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

© 2017 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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.

© 2017 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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.

©2020 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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.

©2019 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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 their 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.

©2019 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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.

© 2020 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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 yardstick 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.

© 2020 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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.

© 2018 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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.

© 2019 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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 full text of The Sedona Conference *Commentary on Data Privacy and Security Issues in Mergers & Acquisitions Practice* is available free for individual download from The Sedona Conference website at: https://thesedonaconference.org/publication/Commentary_on_Data_Privacy_and_Security_Issues_in_Mergers_and_Acquisitions_Practice.

© 2019 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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*, Public Comment Version, is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Enforceability_in_US_Courts_under_GDPR.

© 2021 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

The Sedona Conference Commentary on a Reasonable Security Test (September 2020 Public Comment Version)

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*, Public Comment Version, is available free for individual download from The Sedona Conference website at

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

© 2020 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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.

© 2017, The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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 Investi-

gation, and the privacy and data protection interests 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.

© 2018, The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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.

© 2020 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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, both in 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.

©2016 The Sedona Conference. Reprinted courtesy of The Sedona Conference.

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*, Public Comment Version, 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

© 2020 The Sedona Conference. Reprinted courtesy of The Sedona Conference.