

The Sedona Conference[®]

Working Group One on Electronic Document Retention and Production (WG1)

The Sedona Conference[®] is a nonprofit, 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. Through a combination of Conferences, Working Groups, and the "magic" of dialogue, The Sedona Conference[®] seeks to move the law forward in a reasoned and just way. The Sedona Conference[®] succeeds through the generous contributions of time by its faculties and Working Group members, and is able to fund its operations primarily through the financial support of its members, conference registrants, and sponsorships.

The Sedona Conference[®] Working Group Series is a series of think-tanks consisting of leading jurists, lawyers, experts and consultants brought together by a desire to address various "tipping point" issues in each area under consideration. We have Working Groups up and running in all three areas of our focus (antitrust law, complex litigation and intellectual property rights), and the output of our Working Groups is frequently submitted for peer review at our Regular Season Conferences, other legal education programs and otherwise. We created the Working Group Series Membership Program to allow all interested people to participate in the process through the provision of early input to Working Group drafts, and access to Members Only postings and Discussion Forums. Membership is open to all, and free to full-time government employees.

Working Group One on Electronic Document Retention and Production was formed in October 2002 with the charge to develop "principles and best practices recommendations for electronic document retention and production." Its most influential work product is *The Sedona Principles for Electronic Document Production*, which was first released for public comment in July 2003. In its first few months, it was cited in the landmark *Zubulake* decision on e-discovery and by the Advisory Committee on Rules of Civil Procedure of the Judicial Conference of the United States in their deliberation on proposed rule amendments.

During 2007, *The Sedona Principles* and *The Sedona Guidelines* were updated in light of the new Federal Rules of Civil Procedure and case law developments. WG1 also released commentaries on Legal Holds, Email Management and Archiving, and Search and Retrieval Methods. The Annotated version of *The Sedona Principles* (Second Edition), with citations to more than 1,000 state and federal judicial opinions, was published by BNA. Drafting groups are currently working on commentaries on Legacy Data, Preservation of "Not Reasonably Accessible" Electronically Stored Information, Protecting Privilege and Work Product, Discovery of Electronically Stored Information Held by Non-Parties, E-Discovery Process and Performance Management, and Authentication and Admissibility of Electronic Evidence.

All publications of The Sedona Conference[®] Working Group Series are available free for personal download and use from The Sedona Conference[®] web site, <http://www.thesedonaconference.org>. The most recent publications are listed on the opening page, and all publications are listed under the "Publications" tab. We urge you visit the web site, explore the resources, and consider joining Working Group One.

Copyright © 2008, The Sedona Conference[®]

The Sedona Principles for Electronic Document Production

Second Edition

1. Electronically stored information is potentially discoverable under Fed. R. Civ. P. 34 or its state equivalents. Organizations must properly preserve electronically stored information that can reasonably be anticipated to be relevant to litigation.
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)(2)(C) and its state equivalents, which require consideration of the technological feasibility and realistic costs of preserving, retrieving, reviewing, and producing electronically stored information, as well as the nature of the litigation and the amount in controversy.
3. Parties should confer early in discovery regarding the preservation and production of electronically stored information when these matters are at issue in the litigation and seek to agree on the scope of each party's rights and responsibilities.
4. Discovery requests for electronically stored information should be as clear as possible, while responses and objections to discovery should disclose the scope and limits of the production.
5. The obligation to preserve electronically stored information requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant electronically stored information.
6. Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information.
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.
8. The primary source of electronically stored information for production should be active data and information. Resort to disaster recovery backup tapes and other sources of electronically stored information that are not reasonably accessible requires the requesting party to demonstrate need and relevance that outweigh the costs and burdens of retrieving and processing the electronically stored information from such sources, including the disruption of business and information management activities.
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.
10. A responding party should follow reasonable procedures to protect privileges and objections in connection with the production of electronically stored information.
11. A responding party may satisfy its good faith obligation to preserve and produce relevant electronically stored information by using electronic tools and processes, such as data sampling, searching, or the use of selection criteria, to identify data reasonably likely to contain relevant information.
12. Absent party agreement or court order specifying the form or forms of production, production should be made in the form or forms in which the information is ordinarily maintained or in a reasonably usable form, taking into account the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, search, and display the information as the producing party where appropriate or necessary in light of the nature of the information and the needs of the case.
13. Absent a specific objection, party agreement or court order, the reasonable costs of retrieving and reviewing electronically stored information should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information may be shared by or shifted to the requesting party.
14. Sanctions, including spoliation findings, should be considered by the court only if it finds that there was a clear duty to preserve, a culpable failure to preserve and produce relevant electronically stored information, and a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

The Sedona Guidelines for Managing Information & Records in The Electronic Age

1. **An organization should have reasonable policies and procedures for managing its information and records.**
 - a. Information and records management is important in the electronic age.
 - b. The hallmark of an organization's information and records management policies should be reasonableness.
 - c. Defensible policies need not mandate the retention of all information and documents.

2. **An organization's information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization.**
 - a. No single standard or model can fully meet an organization's unique needs.
 - b. Information and records management requires practical, flexible and scalable solutions that address the differences in an organization's business needs, operations, IT infrastructure and regulatory and legal responsibilities.
 - c. An organization must assess its legal requirements for retention and destruction in developing an information and records management policy.
 - d. An organization should assess the operational and strategic value of its information and records in developing an information and records management program.
 - e. A business continuation or disaster recovery plan has different purposes from those of an information and records management program.

3. **An organization need not retain all electronic information ever generated or received.**
 - a. Destruction is an acceptable stage in the information life cycle; an organization may destroy or delete electronic information when there is no continuing value or need to retain it.
 - b. Systematic deletion of electronic information is not synonymous with evidence spoliation.
 - c. Absent a legal requirement to the contrary, organizations may adopt programs that routinely delete certain recorded communications, such as electronic mail, instant messaging, text messaging and voice-mail.
 - d. Absent a legal requirement to the contrary, organizations may recycle or destroy hardware or media that contain data retained for business continuation or disaster recovery purposes.
 - e. Absent a legal requirement to the contrary, organizations may systematically delete or destroy residual, shadowed or deleted data.
 - f. Absent a legal requirement to the contrary, organizations are not required to preserve metadata.

4. **An organization adopting an information and records management policy should also develop procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.**
 - a. Information and records management policies must be put into practice.
 - b. Information and records management policies and practices should be documented.

- c. An organization should define roles and responsibilities for program direction and administration within its information and records management policies.
- d. An organization should guide employees regarding how to identify and maintain information that has a business purpose or is required to be maintained by law or regulation.
- e. An organization may choose to define separately the roles and responsibilities of content and technology custodians for electronic records management.
- f. An organization should consider the impact of technology (including potential benefits) on the creation, retention and destruction of information and records.
- g. An organization should recognize the importance of employee education concerning its information and records management program, policies and procedures.
- h. An organization should consider conducting periodic compliance reviews of its information and records management policies and procedures, and responding to the findings of those reviews as appropriate.
- i. Policies and procedures regarding electronic management and retention should be coordinated and/or integrated with the organization's policies regarding the use of property and information, including applicable privacy rights or obligations.
- j. Policies and procedures should be revised as necessary in response to changes in workforce or organizational structure, business practices, legal or regulatory requirements and technology.

5. An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigation or audit.

- a. An organization must recognize that suspending the normal disposition of electronic information and records may be necessary in certain circumstances.
- b. An organization's information and records management program should anticipate circumstances that will trigger the suspension of normal destruction procedures.
- c. An organization should identify persons with authority to suspend normal destruction procedures and impose a legal hold.
- d. An organization's information and records management procedures should recognize and may describe the process for suspending normal records and information destruction and identify the individuals responsible for implementing a legal hold.
- e. Legal holds and procedures should be appropriately tailored to the circumstances.
- f. Effectively communicating notice of a legal hold should be an essential component of an organization's information and records management program.
- g. Documenting the steps taken to implement a legal hold may be beneficial.
- h. If an organization takes reasonable steps to implement a legal hold, it should not be held responsible for the acts of an individual acting outside the scope of authority and/or in a manner inconsistent with the legal hold notice.
- i. Legal holds are exceptions to ordinary retention practices and when the exigency underlying the hold no longer exists (*i.e.*, there is no continuing duty to preserve the information), organizations are free to lift the legal hold.



The Sedona Conference[®]

Best Practices for the Selection of Electronic Discovery Vendors: Navigating the Vendor Proposal Process

This paper is an outgrowth of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1), and represents the work of its RFP+ Group: a panel of users of electronic discovery vendor services (two from defense firms, two from plaintiff firms, one from a corporate law department, and one consultant/attorney) with input from the RFP+ Vendor Panel, a group of over 35 electronic discovery vendors who signed up as members to support this effort in response to an open invitation. The goal of the RFP+ Group and this paper is to outline an approach to the selection of an electronic discovery vendor that allows the user to compare apples to apples, to the extent feasible, which makes it easier for all parties to the process to better understand the nature, cost and impact of what is being discussed, in the belief that an informed market will lead to reduced transaction costs, more predictable outcomes, and better business relationships.

The paper includes an explanation of the range of services offered by electronic discovery vendors; scoping the electronic discovery project; the use of Requests for Information (RFIs) to narrow the list of potential vendors; researching vendor background, security, and conflicts; crafting Requests for Proposals (RFPs); and constructing an appropriate matrix for decision-making. Appendices include a RFI and RFP based on a hypothetical fact pattern, non-disclosure agreement, pricing models, and a sample decision matrix. The purpose of the examples is not to provide cookie-cutter forms, but to provide the reader with tools to craft an approach best suited for the needs of a particular case.

This 84-page paper is available free for individual non-commercial use from The Sedona Conference[®], <http://www.thesedonaconference.org>.

*Copyright © 2008, The Sedona Conference[®].
Reprinted courtesy of The Sedona Conference[®].*

*The full text of this Commentary is available free for personal use from
The Sedona Conference[®] website at www.thesedonaconference.org*

E-Discovery and Digital Information Management (Second Edition, 2007)

This authoritative 59-page Glossary is an outgrowth of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1) and represents the work of its RFP+ Group: a panel of users of electronic discovery vendor services (two from defense firms, two from plaintiff firms, one from a corporate law department, and one consultant/attorney) with input from the RFP+ Vendor Panel, a group of over 35 electronic discovery vendors who signed up as members to support this effort in response to an open invitation, and significant input from the public since the first edition was published in 2005. The goal is to create a common language to facilitate the process of communication between client and counsel, between counsel and e-discovery product and service vendors, between opposing counsel negotiating the scope and conduct of e-discovery. It has also been cited in law review articles and by state and federal courts in ediscovery decisions.

The Glossary defines more than 500 e-discovery terms, from **ablate**¹ to **zettabyte**², including such commonly used (and often misused) terms as **deletion**³ and **metadata**⁴.

*Copyright © 2008, The Sedona Conference[®].
Reprinted courtesy of The Sedona Conference[®].*

*The full text of the Glossary is available free for personal use from
The Sedona Conference[®] web site at www.thesedonaconference.org.*

¹ “**Ablate**: Describes the process by which laser-readable ‘pits’ are burned into the recorded layer of optical discs, DVD-ROMs and CD-ROMs.”

² “**Zettabyte**: 1,180,591,620,717,411,303,424 bytes - 1024⁷ (a sextillion bytes). *See* Byte.”

³ “**Deletion**: Deletion is the process whereby data is removed from active files and other data storage structures on computers and rendered inaccessible except through the use of special data recovery tools designed to recover deleted data. Deletion occurs on several levels in modern computer systems: (a) File level deletion renders the file inaccessible to the operating system and normal application programs and marks the storage space occupied by the file’s directory entry and contents as free and available to re-use for data storage, (b) Record level deletion occurs when a record is rendered inaccessible to a database management system (DBMS)(usually marking the record storage space as available for re-use by the DBMS, although in some cases the space is never reused until the database is compacted) and is also characteristic of many email systems (c) Byte level deletion occurs when text or other information is deleted from the file content (such as the deletion of text from a word processing file); such deletion may render the deleted data inaccessible to the application intended to be used in processing the file, but may not actually remove the data from the file’s content until a process such as compaction or rewriting of the file causes the deleted data to be overwritten.”

⁴ “**Metadata**: Data typically stored electronically that describes characteristics of ESI, found in different places in different forms. Can be supplied by applications, users or the file system. Metadata can describe how, when and by whom ESI was collected, created, accessed, modified and how it is formatted. Can be altered intentionally or inadvertently. Certain metadata can be extracted when native files are processed for litigation. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed to paper or electronic image. *See also* Application Metadata, Document Metadata, Email Metadata, Embedded Metadata, File System Metadata, User-Added Metadata and Vendor-Added Metadata. For a more thorough discussion, see *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* (Second Edition).”

The Sedona Conference[®] Commentary on Legal Holds: The Trigger & The Process

Information is the lifeblood of the modern world, a fact that is at the core of our litigation discovery system. The law has developed rules regarding the manner in which information is to be treated in connection with litigation. One of the principal rules is that whenever litigation is reasonably anticipated, threatened or pending against an organization that organization has a duty to preserve relevant information. This duty arises at the point in time when litigation is reasonably anticipated whether the organization is the initiator or the target of litigation.

The duty to preserve information includes an obligation to identify, locate, and maintain, information that is relevant to specific, predictable, and identifiable litigation. When preservation of electronically stored information (“ESI”) is required, the duty to preserve supersedes records management policies that would otherwise result in the destruction of ESI. A “legal hold” program defines the processes by which information is identified, preserved, and maintained when it has been determined that a duty to preserve has arisen.

The basic principle that an organization has a duty to preserve relevant information in anticipation of litigation is easy to articulate. However, the precise application of that duty can be elusive. Every day, organizations apply the basic principle to real-world circumstances, confronting the issue of when the obligation is triggered and, once triggered, what is the scope of the obligation. This 24-page Commentary, intended to provide guidance on those issues, is divided into two parts: The “trigger” and the “process.”

Part I addresses the trigger issue and provides practical guidelines for making a determination as to when the duty to preserve relevant information arises. What should be preserved and how the preservation process should be undertaken including the implementation of legal holds is addressed in Part II. The keys to addressing these issues are reasonableness and good faith. The guidelines are intended to facilitate reasonable and good faith compliance with preservation obligations. The guidelines are meant to provide the framework an organization can use to create its own preservation procedures. In addition to the guidelines, suggestions as to best practices are provided along with several illustrations as to how the guidelines and best practices might be applied under hypothetical factual situations.

Guideline 1: Reasonable anticipation of litigation arises when an organization is on notice of a credible threat it will become involved in litigation or anticipates taking action to initiate litigation.

Guideline 2: The adoption and consistent implementation of a policy defining a document retention decision-making process is one factor that demonstrates reasonableness and good faith in meeting preservation obligations.

Guideline 3: The use of established procedures for the reporting of information relating to a potential threat of litigation to a responsible decision maker is a factor that demonstrates reasonableness and good faith in meeting preservation obligations.

Guideline 4: The determination of whether litigation is reasonably anticipated should be based on good faith, reasonableness, a reasonable investigation and an evaluation of the relevant facts and circumstances.

Guideline 5: Judicial evaluation of a legal hold decision should be based on the good faith and reasonableness of the decision (including whether a legal hold is necessary and how the legal hold should be executed) at the time it was made.

The Sedona Conference[®] Commentary on Legal Holds: The Trigger & The Process cont.

- Guideline 6:** When a duty to preserve arises, reasonable steps should be taken to identify and preserve relevant information as soon as is practicable. Depending on the circumstances, a written legal hold (including a preservation notice to persons likely to have relevant information) should be issued.
- Guideline 7:** In determining the scope of information that should be preserved, the nature of the issues raised in the matter, experience in similar circumstances and the amount in controversy are factors that may be considered.
- Guideline 8:** A legal hold is most effective when it:
- (a) Identifies the persons who are likely to have relevant information and communicates a preservation notice to those persons;
 - (b) Communicates the preservation notice in a manner that ensures the recipients will receive actual, comprehensible and effective notice of the requirement to preserve information;
 - (c) Is in written form;
 - (d) Clearly defines what information is to be preserved and how the preservation is to be undertaken;
 - (e) Is periodically reviewed and, when necessary, reissued in either its original or an amended form.
- Guideline 9:** The legal hold policy and process of implementing the legal hold in a specific case should be documented considering that both the policy and the process may be subject to scrutiny by the opposing party and review by the court.
- Guideline 10:** The implementation of a legal hold should be regularly monitored to ensure compliance.
- Guideline 11:** The legal hold process should include provisions for the release of the hold upon the termination of the matter at issue.

*Copyright © 2008, The Sedona Conference[®]
Reprinted courtesy of The Sedona Conference[®]*

*The full text of this Commentary is available free for individual download from
The Sedona Conference[®] web site at www.thesedonaconference.org.*



The Sedona Conference[®] Commentary on ESI Evidence & Admissibility

During the last decade, culminating with the adoption of significant amendments to the Federal Rules of Civil Procedure (“FRCP”) on December 1, 2006, the legal community has expended significant energy and focus on electronic data. A main focus has been on whether and under what circumstances a litigant must provide such data – known more formally as electronically stored information or “ESI” – to an adverse party.

While there are still significant issues to resolve with the amended FRCP and electronic discovery, the legal community is also grappling with whether and how ESI, once produced, can actually be authenticated and used as evidence at trial or in motion practice. As succinctly noted by Judge Grimm in a recent, leading case on the subject:

[C]onsidering the significant costs associated with discovery of ESI, it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted.

Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007).

This 28-page Commentary focuses specifically on that concern, and is divided into three parts: Part I is a brief survey of the applicability and application of existing evidentiary rules and case law addressing the same. Part II addresses new issues and pitfalls that are looming on the horizon. Part III provides practical guidance on the use of ESI in depositions and in court.

*Copyright © 2008, The Sedona Conference[®].
Reprinted courtesy of The Sedona Conference[®].*

*The full text of this Commentary is available free for personal use from
The Sedona Conference[®] web site at www.thesedonaconference.org.*



The Sedona Conference[®] Commentary on Non-Party Production & Rule 45 Subpoenas

The December 2006 amendments to the Federal Rules of Civil Procedure relating to electronically stored information (“ESI”) affected not only discovery practices between parties, but also the acquisition of information from non-parties. This 25-page Commentary describes the changes to Federal Rule of Civil Procedure 45 (third party subpoenas), briefly explains the similarities and differences between amended Rule 45 and amended Rules 26, 34 and 37, and explores what lessons the case law teaches as to whether there are differences in the way courts address the duties of parties and non-parties related to producing ESI. In addition to discussing what the new rules and cases require, the Commentary explores the actual experiences of attorneys and parties and outline best practices.

*Copyright © 2008, The Sedona Conference[®].
Reprinted courtesy of The Sedona Conference[®].*

*The full text of this Commentary is available free for personal use from
The Sedona Conference[®] web site at www.thesedonaconference.org.*

on the Use of Search and Retrieval Methods in E-Discovery

This Commentary is an outgrowth of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1) and represents the work of its Search and Retrieval Sciences Special Project Team, consisting of a diverse group of lawyers and representatives of firms providing consulting and legal services to the legal community. The mission has been to explore the nature of the search and retrieval process in the context of civil litigation and regulatory compliance in the digital age. The goal is to provide the bench and bar with an educational guide to an area of e-discovery law that we believe will only become more important over time, given the need to accurately and efficiently search for relevant information contained within the exponentially increasing volumes of electronically stored information (ESI) that are subject to litigation, investigations, and regulatory activities.

The findings of the Special Project Team are summarized in eight Practice Points, explained and developed in the 38-page Commentary:

Practice Point 1. In many settings involving electronically stored information, reliance solely on a manual search process for the purpose of finding responsive documents may be infeasible or unwarranted. In such cases, the use of automated search methods should be viewed as reasonable, valuable, and even necessary.

Practice Point 2. Success in using any automated search method or technology will be enhanced by a well thought out process with substantial human input on the front end.

Practice Point 3. The choice of a specific search and retrieval method will be highly dependent on the specific legal context in which it is to be employed.

Practice Point 4. Parties should perform due diligence in choosing a particular information retrieval product or service from a vendor.

Practice Point 5. The use of search and information retrieval tools does not guarantee that all responsive documents will be identified in large data collections, due to characteristics of human language. Moreover, differing search methods may produce differing results, subject to a measure of statistical variation inherent in the science of information retrieval.

Practice Point 6. Parties should make a good faith attempt to collaborate on the use of particular search and information retrieval methods, tools and protocols (including as to key words, concepts, and other types of search parameters).

Practice Point 7. Parties should expect that their choice of search methodology will need to be explained, either formally or informally, in subsequent legal contexts (including in depositions, evidentiary proceedings, and trials).

Practice Point 8. Parties and the courts should be alert to new and evolving search and information retrieval methods.

*Copyright © 2008, The Sedona Conference[®].
Reprinted courtesy of The Sedona Conference[®].*

*The full text of this Commentary is available free for personal use from
The Sedona Conference[®] web site at www.thesedonaconference.org.*



The Sedona Conference[®] Commentary on Email Management:

Guidelines for the Selection of a Retention Policy

Electronic mail (“Email”) is of vital importance to the productive efforts of an enterprise and its use is growing exponentially. In 2005, the average user processed 75 e-mails a day and the Radicata Group estimates that corporate e-mail traffic per user has increased at a rate of 33% per year since then. Projections are that worldwide traffic in 2006 was at the rate of 183 billion messages per day. Many organizations are struggling to decide how best to cope with the explosion of email while reconciling competing needs imposed by business, regulatory and litigation requirements. This Commentary suggests Guidelines for determining the core elements of an email retention policy suitable for public and private entities. Although the legal, regulatory and cultural environments of each organization vary greatly, there are common elements to a legally defensible email management policy. In our Working Group discussions, we have been struck by the fact that entities of comparable size with similar legal risk and regulatory profiles can and do successfully adopt different retention strategies and that these strategies can vary over time, depending upon the phase of development, the size and complexity of the organization, and the particular issues most significant to the entity at any particular time.

The key is to develop and enforce in good faith those reasonable policies that best fit the entity. Four basic Guidelines are presented and explored in depth in this 14-page Commentary, followed by an Appendix including a flow chart of the decision making process and describing to contrasting retention strategies that can be followed.

*Copyright © 2008, The Sedona Conference[®].
Reprinted courtesy of The Sedona Conference[®].*

*The full text of this Commentary is available free for personal use from
The Sedona Conference[®] web site at www.thesedonaconference.org.*