



THE SEDONA CONFERENCE® COMMENTARY ON:

*Preservation, Management and
Identification of Sources of Information
that are Not Reasonably Accessible*

A Project of The Sedona Conference®
Working Group on Electronic Document
Retention & Production (WG1)

JULY 2008



The Sedona Conference®
Commentary on

*Preservation, Management and Identification of
Sources of Information that are Not Reasonably
Accessible*

A Project of The Sedona Conference®
Working Group on Electronic
Document Retention & Production (WG1)

July 2008

Editors:

Thomas Y. Allman
William P. Butterfield
Matthew Hagarty
Cecil A. Lynn III
Jon A. Neiditz
Maureen O'Neill
Ira P. Rothken
Peter B. Sloan

REPRINT REQUESTS:

Requests for reprints or reprint information should be directed to
Richard Braman, Executive Director of The Sedona Conference, at
tsc@sedona.net or 1-866-860-6600.

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of
the members of The Sedona Conference® Working Group 1.

They do not necessarily represent the views of any of the individual participants or their employers,
clients, or any other organizations to which any of the participants belong nor do they necessarily
represent official positions of The Sedona Conference®.

* This Commentary was the subject of dialogue at three Working Group Meetings,
and many Working Group Members submitted comments and edits as well.

Thanks go to all who participated in the dialogue that led to this Commentary.

In addition, we thank all of our Working Group SeriesSM Sustaining and Annual Sponsors, whose support is
essential to our ability to develop Working Group Series publications.

For a listing of our sponsors just click on the "Sponsors" Navigation bar on the homepage of our website.



Preface

This Sedona Conference® Commentary focuses on the decision making process relating to the preservation of sources of electronically stored information that may contain discoverable information that is “not reasonably accessible.”¹ The “reasonable accessibility” distinction - introduced by the 2006 Federal E-Discovery Amendments as part of the “two-tiered” approach to discovery - plays a role in, but is not wholly determinative of, preservation obligations.

The central dilemma of preservation planning in the absence of the opportunity to discuss discovery requests or reach prior agreement among the parties is predicting exactly which sources of information may actually be discoverable in a given case. No bright-lines exist.² The primary duty is to make reasonable assessments in good faith.³

To assist litigants and the courts, we have developed the following Guidelines that summarize our recommendations for making those assessments.⁴ The Guidelines also discuss how parties may “identify” inaccessible sources that will not be preserved and emphasize the value of cooperative efforts to reach agreements on preservation topics in dispute that reflect the unique demands of each case.

The Guidelines are:

Guideline 1. Where litigation is anticipated but no plaintiff has emerged or other considerations make it impossible to initiate a dialogue, the producing party should make preservation decisions by a process conforming to that set forth in the Decision Tree in Figure 1.

Guideline 2. As soon as feasible, preservation issues should be openly and cooperatively discussed in sufficient detail so the parties can reach mutually satisfactory accommodation and also evaluate the need, if any, to seek court intervention or assistance.

Guideline 3. In conjunction with the initial discussions or where appropriate in the response to discovery requests, parties should clearly identify the inaccessible sources reasonably related to the discovery or claims which are not being searched or preserved.

Guideline 4. A party should exercise caution when it decides for business reasons to move potentially discoverable information subject to a preservation duty from accessible to less accessible data stores.

Guideline 5. It is acceptable practice, in the absence of an applicable preservation duty, for entities to manage their information in a way that minimizes accumulations of inaccessible data, provided that adequate provisions are made to accommodate preservation imperatives.

¹ Rule 26(b)(2)(B) defines sources that are “reasonably accessible” as being so because of “undue burden or cost.” For convenience of reference, sources of this type are sometimes referred to herein as “inaccessible sources.”

² The Advisory Committee decided that federal rulemaking should focus on mandating early discussion of preservation “issues” while providing targeted guidance [Rule 37(e)] for courts facing motions for sanctions.

³ *Texas v. City of Frisco*, 2007 WL 828055 (E.D. Tex. March 27, 2008) (“[W]hile they do not specifically address pre-suit litigation hold requests, the Rules of Civil Procedure contemplate that the parties will act in good faith in the preservation and production of documents. See Fed. R. Civ. P. 37.”).

⁴ In some circumstances, the intentional destruction of potentially relevant evidence can lead to criminal prosecution. See, e.g., 18 U.S.C. §§ 1512(c) and 1519. While this paper is not intended to address the criminal consequences of failing to preserve relevant evidence, it may be of analytical assistance to those dealing with criminal matters.

Guideline 6. An entity should encourage appropriate cooperation among legal and other functions and business units within the organization to help ensure that preservation obligations are met and that resources are effectively utilized.

Introduction

The 2006 Amendments to the Federal Rules of Civil Procedure provide that electronically stored information that is not reasonably accessible because of undue burden or cost need not be reviewed or produced in discovery absent agreement or an order issued for “good cause, considering the limitations of Rule 26(b)(2)(C).”⁵ Rule 26(b)(2)(B) also requires that a party “identify” those sources it does not intend to search or from which discovery will not be made.

The Amendments are *not*, however, the source of pre-discovery obligations to preserve potential sources of discoverable electronically stored information, a task left to the common law.⁶ The duty to preserve applies to any and all relevant documents, tangible things, or electronic information in the possession, custody, or control of a party⁷ no matter where located. The knowledge or belief that litigation has begun or is imminent “triggers” preservation obligations and requires that reasonable steps be undertaken to maintain relevant and discoverable information pending discovery,⁸ including third party discovery.⁹

The Committee Notes to Rules 26(b)(2) and Rule 37(e) make clear that preservation obligations may apply even when electronically stored information is located on an inaccessible source. The Note to Rule 26(b)(2) provides that “[a] party’s identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence.” Moreover, the Note to Rule 37(e) instructs that parties may not “exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve.”¹⁰

⁵ Rule 26(b)(2)(C) contains the “proportionality” limitations added in 1983 and formerly found in Rule 26(b)(2). See Wright and Miller, “Inaccessible” Electronically Stored Information, 8 Fed. Prac. & Proc. Civ. 2d § 2008.2 (2007).

⁶ See *Silvestri v. GM*, 271 F.3d 583 (4th Cir. 2001).

⁷ See *Leon v. IDX Systems*, 464 F.3d 951, 955-957, 961 (9th Cir. Sept. 2006) (upholding sanction against a terminated whistleblower plaintiff who had deleted data from his company-furnished laptop).

⁸ See *The Sedona Conference® Commentary on Legal Holds: The Trigger & The Process* (August 2007 Public Comment Version, www.thesedonaconference.org) 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”).

⁹ See *The Sedona Conference® Commentary on Non-Party Production and Rule 45 Subpoenas* (March 2008 Public Comment Version, www.thesedonaconference.org), at pp 3-4, citing *In re Napster, Inc. Copyright Litigation*, 2006 WL 305086 at *6 (N.D. Cal. Oct. 25, 2006) (service of and compliance with a non-party subpoena is not necessarily sufficient notice of future litigation).

¹⁰ A producing party can face a Hobson’s choice between the burden and cost of preservation and the risk of sanctions for failing to do so. Parties engaged in ongoing, recurrent litigation can also face a serial preservation duty dilemma, in which preserved data sources that would not be kept for any other reason may become subject to preservation duties in subsequent litigation.

Preservation Obligations

It has been left to the case law and best practice guidelines such as *The Sedona Principles* to provide *de facto* “national standards” for preservation obligations in the absence of party agreement. Principle 5, for example, provides that implementation of preservation duties requires “reasonable and good faith efforts,” but that it is “unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.” Comments 5.c. and 5.d. to Principle 5 recommend use of a “repeatable, documented” process in implementing “legal” or “litigation” holds, a topic that is the subject of *The Sedona Conference® Commentary on Legal Holds: The Trigger & The Process*.¹¹

This approach is representative of the evolving case law¹² and is buttressed by Principle 6, which provides that responding parties are “best situated” to evaluate the detailed procedures, methodologies and technologies “appropriate for preserving and producing their own electronic data and documents.” As noted in *Zubulake v. UBS Warburg* (“*Zubulake IV*”), “[because] there are many ways to manage electronic data, litigants are free to choose how this task [preservation] is accomplished.”¹³

The best way to avoid post-production preservation disputes is by developing early agreement on contentious preservation issues through transparent and cooperative efforts. However, there will be instances when preservation decisions will be required in advance of the opportunity to develop such understandings or seek court guidance. Under those circumstances, a party should act in a reasonable and good faith manner¹⁴ based on its best understanding of that which is likely to be needed in discovery.

To help guide this process, we recommend:

Guideline 1. *Where litigation is anticipated but no plaintiff has emerged or other considerations make it impossible to initiate a dialogue, the producing party should make preservation decisions by a process conforming to that set forth in the Decision Tree in Figure 1 and as described above.*

Working Group 1 has developed a multi-step approach to preservation decisions, which is equally applicable to all sources of information, whether accessible or inaccessible.¹⁵ This logical approach is graphically portrayed in the Decision Tree in Figure 1 below. In summary:

The initial step requires an initial assessment of what type of information would be relevant and discoverable, based on what is then known, much as is done in assessing the scope of a litigation hold. After determining the relevant issues, a party should next assess what potential data sources might reasonably contain that information. To help perform that assessment, the party must attempt to identify custodians who might have created or controlled relevant information, and locate where that information is kept.

¹¹ See *The Sedona Conference® Commentary on Legal Holds: The Trigger & The Process* (August 2007 Public Comment Version), *supra*, Guideline 6 (“Depending on the circumstances, a written legal hold (including a preservation notice to persons likely to have relevant information) should be issued.”).

¹² See *Miller v. Holzmann*, 2007 WL 172327 (D. D.C. Jan. 17, 2007) (holding that *Sedona Principle 5* is reasonable and in accordance with developing case law).

¹³ 220 F.R.D. 212, 218 (Oct. 22, 2003).

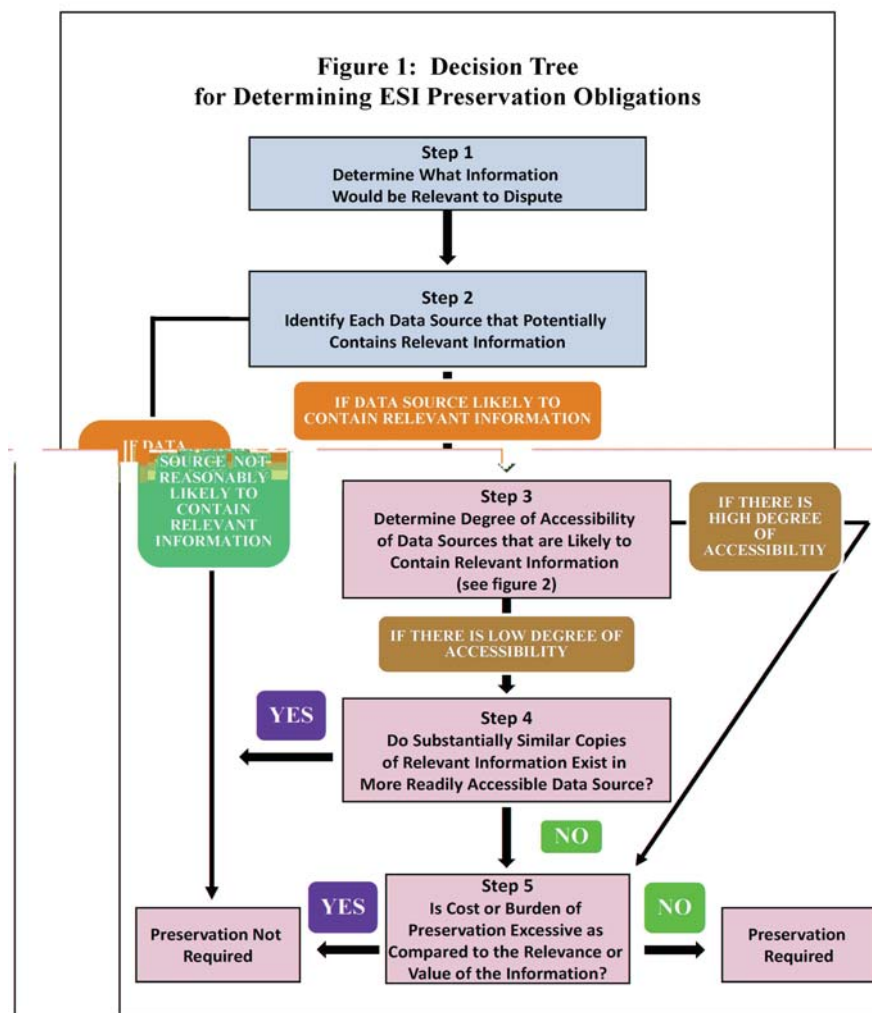
¹⁴ Rule 37(e), as renumbered after the 2007 Style Amendments, provides that in the absence of exceptional circumstances, rule-based sanctions should not issue “for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.” See *Escobar v. City of Houston*, 2007 WL 2900581 at *18 (S.D. Tex. Sept. 27, 2007) (applying rule in context of recycling of audio tapes).

¹⁵ See, e.g., *Wm T. Thompson v. General Nutrition Corporation*, 593 F. Supp. 1443, 1455 (C.D. Cal. Sept. 28, 1984) (“While a litigant is under no duty to keep or retain every document in its possession once a complaint is filed, it is under a duty to preserve what it knows, or reasonably should know, is relevant to the actions, is reasonably calculated to lead to the discovery admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request.”).

Based on that preliminary analysis, the party should then assess whether each identified data source contains potentially discoverable information, taking into account what is known or knowable at the time about the potential discovery. If a party is neither actually aware nor should be aware of that possibility, there is no obligation to preserve the source. However, if the opposite is true, the next step is to assess the perceived accessibility of the source on which it may be found. If the source in question is not reasonably accessible, it may nonetheless still have to be preserved if the producing party does not have a reasonable belief that the information is available on other, more accessible sources.

However, whether the source is readily accessible or not, the Decision Tree makes it clear that the accessibility assessment is not the final word. As a fifth and final step, only when the perceived benefit to discovery of the information is not outweighed by the burdens and costs involved is preservation required. This “proportionality” analysis is similar to the familiar principles, which courts use in determining production from such sources.¹⁶

The Decision Tree is set forth below in Figure 1:



¹⁶ By way of analogy from the production context, *See* Ronald J. Hedges, *Judges, Lawyers, and the New Rules*, 43 TRIAL 20, 22 (Apr. 2007) (“[I]n the end, we have to use the same test to determine whether discovery should go forward – the so-called proportionality rule, which had been Rule 26(b)(2) and is now 26(b)(2)(C). That rule provides that a judge can deny or limit or condition a discovery request that is too burdensome or expensive.”).

This analysis - which has necessarily been simplified for ease of explanation – is based in large measure on principles that emerged before, and which were clarified by, the 2006 Amendments.

We turn now to a more detailed discussion of each these steps in the Decision Tree.

Step One Analysis - Relevance and Responsiveness

Electronically stored information need not be preserved, absent an agreement or court order, in the absence of a reasonable belief that it is potentially relevant information that is likely to be discoverable in litigation.

An initial question in any preservation analysis is whether the information which may be contained on a source is potentially discoverable in the action. The assessment necessarily depends upon what the potential preserving party knew or reasonably should have known at the time. There will always be sources of information which clearly cannot contain discoverable information because of the origin of the information on the source or the time parameters involved.

In the matter of *In re Kmart Corporation*,¹⁷ for example, there was no evidence Kmart knew that discoverable information existed among email being destroyed pursuant to a preexisting policy. The court rejected the comparison to *Zubulake* as “wishful thinking” because there was no reason to anticipate the need for the information. Similarly, in *Healthcare Advocates v. Harding, Early, Follmer & Frailey*,¹⁸ no duty to retain electronic screen shots was found when the producing party neither “knew or should have known” that temporary cache files would be sought in litigation.¹⁹

Where actual notice of the potential discoverability is lacking, or where the potential relevance is not obvious, efforts by a potential requesting party to provide notice that information should be preserved can become significant. A general demand for preservation is not sufficient, however. For example, in *Frey v. Gainey Transportation Services, Inc.*,²⁰ a fifteen page demand letter was deemed to be “an [ineffectual] effort on the plaintiff’s part to sandbag a defendant in the event that any of those materials were not preserved” where no particularly relevant items were sought.

A requesting party should not ignore the issue. If the requesting party can identify with particularity sources of information that it believes will be relevant and discoverable in the litigation, it should notify the producing party, especially if the relevance of the information is not immediately apparent. *In re Veeco Instruments, Inc. Securities Litigation*,²¹ the court held that it “would be unreasonable for the [requesting party] to assume that back-up tapes were being searched given that . . . no discussions on the subject were held.”²² Similarly, in *Petcou v. C.H. Robinson Worldwide, Inc.*,²³ the court refused to fault a party for failing to impose an entity-wide preservation order on deletion of email where the requesting party had not indicated the need to do so.²⁴

¹⁷ 371 B.R. 823 (Bkrctcy. N.D. Ill. 2007).

¹⁸ 497 F. Supp. 2d 627, 640-41 (E.D. Pa. 2007).

¹⁹ *Id.* at 641 (“[T]hey had no reason to believe that their activities would subject them to a lawsuit for ‘hacking,’ [and the failure to preserve] is not an action that shocks the conscience.”).

²⁰ 2006 WL 2443787 (N.D. Ga. Aug. 22, 2006).

²¹ 2007 WL 983987 (S.D.N.Y. Apr. 2, 2007).

²² *Id.* at *1.

²³ 2008 WL 542684 (N.D. Ga. Feb. 25, 2008) (“It does not appear that Defendant acted in bad faith in following its established policy for retention and destruction of e-mails.”).

²⁴ See also *Marketfare Annunciation, LLC v. United Fire & Casualty Insurance Co.*, 2007 WL 3273440 (E.D. La. Nov. 5, 2007) (refusing to consider a motion for sanctions because the preservation issue should have been raised in a timely manner “as opposed to bypassing this step in the discovery process and seeking sanctions directly.”).

The need for affirmative action is especially true where the nature of the information sought is temporary or ephemeral.

Illustration. In a trade secrets action against defendant involving the theft of a secret formula, plaintiff believes that an employee of defendant received the trade secret on his computer via a non-company authorized, web-based email account. Plaintiff needs screenshots of the email pages and related communications to prove the theft of trade secrets, which can only be secured "forensically" by immediately obtaining the web browsing history found in areas of the operating system where "temp," "cache," and "hidden" files reside, but are constantly and automatically being overwritten. Plaintiff must provide expedient and specific notice to preserve such web e-mail data since the data is not in the company's authorized email server, is inaccessible, and is constantly being overwritten via automated processes.

Thus, in *Columbia Pictures v. Bunnell*,²⁵ the court refused to find a duty to preserve information temporarily residing in RAM where the producing party had no reason to anticipate a request for the information in discovery.²⁶

Another example is where a requesting party fails to raise the need for preservation of metadata pending discovery. As noted in *Kentucky Speedway, LLC v. NASCAR*,²⁷ "whether metadata is relevant or should be produced is [an issue] which ordinarily should be addressed by the parties in a Rule 26(f) conference."²⁸

In *O'Bar v. Lowe's Home Centers, Inc.*,²⁹ the court required parties to discuss "whether production will be of the Native File, Static Image, or other searchable or non-searchable formats."³⁰ In *Kentucky Speedway*, the court relied on the failure to raise the topic in early discussions as a reason for refusing a belated attempt to seek metadata.

Step Two Analysis – Identification of Data Sources

After determining the type and nature of information that would be relevant to the dispute, an organization should make reasonable efforts to identify the data sources that potentially contain that information.

Once a party identifies the information that would be relevant to a pending or imminent dispute, it must determine where that information likely resides. This task typically involves identifying (1) the custodians who created or control relevant information and (2) the data sources where the custodians' information resides. This process should be conducted as part of an organization's efforts to implement a legal hold. In the *Commentary on Legal Holds*, The Sedona Conference® has offered guidance:

²⁵2007 WL 2080419 (C.D. Cal. May 29, 2007), *motion to review denied*, 245 F.R.D. 443, 446 (C.D. Cal. 2007) (requiring preservation and future production of information temporarily stored in RAM, which was highly relevant and could be logged with minimal efforts).

²⁶The magistrate judge held that "the defendants' failure to retain the Server Log Data in RAM was based on a good faith belief that preservation of data temporarily stored only in RAM was not legally required" because, *inter alia*, there had been "no specific request by the defendants to preserve Server Log Data present solely in RAM." 2007 WL 2080419, at *14. During a colloquy about the case at an E-Discovery Conference, the point was made by a magistrate judge that there could very well be occasions when the duty to preserve such ephemeral information will be obvious and steps may have to be undertaken to preserve it if the need and relevance outweigh the burdens and costs of doing so (See Figure 1, Decision Tree, Steps Four and Five).

²⁷2006 WL 5097354 (E.D. Ky. Dec. 18, 2006).

²⁸*Id.* at *8 (failure to notify of demand for metadata until seven months after production of electronic and hard copy of documents).

²⁹2007 WL 1299180 (W.D. N.C. May 2, 2007).

³⁰*Id.* at *4 (adapted from the "Suggested Protocol for Discovery of Electronically Stored Information" available at <http://www.mdd.uscourts.gov/news/ESI/Protocol.pdf>).

For large preservation efforts, a process that is planned, systemized and scalable is ideal, while an ad hoc, disjointed and/or manual process can result in undue burden and expense. An example of an inefficient process involves collecting immense amounts of information from every custodian, server and restored back-up tape without any initial effort to identify relevant information. With no means to triage the information and to filter out irrelevant ESI, the collection may be overbroad, with a great deal of irrelevant information aggregated into a central repository where it is then finally processed and searched.³¹

An organization should consider all data sources within its “possession, custody, and control” that are likely to include relevant, unique information.³² This includes data sources within the physical possession of the organization, and other sources within the possession or custody of third parties, pursuant to contractual or other relationships, such as information held by Application Service Providers (ASPs) and other service providers.³³

This assessment will be easier to make for some data sources than for others. For example, information stored in media that requires special restorative efforts to place it in a form where it can be viewed is, by definition, difficult to assess. However, based on knowledge of date ranges, individuals or business units involved, or other features, it may be possible to make reasoned judgments.

Step Three Analysis – Relative Accessibility

The relative accessibility of a source of potentially discoverable information is best evaluated by assessing the burdens involved in viewing, extracting, preserving, and searching the source as well as other relevant factors imposed by the location, including the dispersion and the volumes involved.

The use of “accessibility” of an information source as a differentiator in the Federal Rules can be traced to two important influences.

First, Texas Rule 196.4, adopted in 1999, adopted a distinction between production that required a prior court order and that which did not because the information was available to the producing party in the ordinary course of business.³⁴ Second, the initial *Zubulake* opinion³⁵ adopted the concept of “accessibility” in connection with determining when and whether to allow cost shifting.³⁶

The Advisory Committee adopted elements of both concepts in instituting the “two-tiered” standard for e-discovery production, now found in Rule 26(b)(2)(B), whereby production from inaccessible sources can be ordered only upon a showing of “good cause, considering the limitations of Rule 26(b)(2)(C).”³⁷

³¹ See *The Sedona Conference*® *Commentary on Legal Holds: The Trigger & the Process* (August 2007 Public Comment Version), *supra*, at 11.

³² *Id.*, at 12.

³³ *Id.*

³⁴ See Texas Rule 196.4 (“The responding party must produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business.”).

³⁵ *Zubulake v. UBS Warburg* (“*Zubulake I*”), 217 F.R.D. 309 (S.D.N.Y. May 13, 2003). There have been at least five *Zubulake* decisions. In addition to *Zubulake I*, three others address electronic discovery. See *Zubulake III*, 216 F.R.D. 280 (S.D.N.Y. July 24, 2003); *Zubulake IV*, 220 F.R.D. 212 (S.D.N.Y. Oct. 22, 2003); *Zubulake V*, 229 F.R.D. 422 (S.D.N.Y. July 20, 2004).

³⁶ For a concise summary of the history of cost-shifting before and after the 2006 Amendments, an excellent resource is Mazza et. al, *In Pursuit of FRCP 1: Creative Approaches to Cutting and Shifting the Costs of Discovery of Electronically Stored Information*, 13 Rich. J. L. & Tech. 11 at *99 (Spring 2007)

³⁷ Fed. R. Civ. P. 26(b)(2)(C)(iii) requires that a “court *must* limit the frequency or extent of discovery otherwise allowed by these rules or local rules if it determines [that] “the burden or expense of the proposed discovery outweighs its likely benefit. . . .” (emphasis added). For a discussion of the post-Amendment decisions applying these principles to inaccessible sources, see Thomas Y. Allman, *The ‘Two-Tiered’ Approach to E-Discovery: Has Rule 26(B)(2)(b) Fulfilled Its Promise*, 14 Rich. J. L. & Tech. 7 (Spring 2008).

The Federal Rules do not define “not reasonably accessible” other than to caution that it turns on the presence or absence of “undue burden or cost.” Under the emerging case law at the time of the 2006 Amendments, there was a reasonable consensus, as outlined in the introductory remarks in the 2005 Advisory Committee Report,³⁸ that the following data types were often deemed not to be reasonably accessible without undue burden or cost:

- information on databases whose retrieval cannot be quickly accomplished because the database software is not capable of extracting the information sought without substantial additional programming;
- information stored on media that must be transformed into another form before search and retrieval can be achieved;
- deleted information whose fragments remain only accessible by forensics; and
- legacy data remaining from obsolete systems that is unintelligible on successor systems.

As noted in the Decision Tree, and as the Advisory Committee made clear, the inaccessibility of a potential source, in and of itself, does not determine whether it must be preserved, which depends on the facts of each case (See Decision Tree, Steps 4 and 5).

In an effort to assist in the analysis of relative accessibility as called for in Step 3, Sedona has identified twelve factors which should be considered, as set forth in Figure 2 below entitled the “Sedona Accessibility NRA Factors.” These factors include both *Media Based Factors* and *Data Complexity Factors*.

A. Media Based Factors

The Media Based Factors (Numbers 1-6, Figure 2) are alternative categories of storage media, arranged in descending orders of accessibility, as inspired by *Zubulake I*,³⁹ a pre-2006 Amendment decision which used the “reasonably accessible” concept for other purposes. In *Zubulake I*, the court found that the time and expense required to retrieve documents and electronic data depends primarily on whether such information “is kept in an accessible or inaccessible format ...[and] [w]hether electronic data is accessible or inaccessible turns largely on the media on which it is stored.”⁴⁰

Zubulake I broke down electronic data into five categories, (1) active on-line data (hard drives, for example); (2) near-line data (typically, robotic storage devices such as optical disks); (3) offline storage/archives (removable optical disks or magnetic tape media which can be labeled and stored in a shelf or rack); (4) backup tapes (devices like tape recorders that read data from and write it onto a tape in a manner typically not organized for retrieval of individual documents or files); and (5) erased, fragmented or damaged data (such data can only be accessed after significant processing).⁴¹ The first three categories of media types were considered by the Court to be “accessible” and the last two categories were considered inaccessible.

The first six Sedona Accessibility Factors (See Figure 2) correspond to the media based categories from *Zubulake I*, with the exception that the fifth category from that decision has been subdivided by Sedona for ease of use.⁴²

³⁸ See Final Report, Standing Committee (2005) at C-42.

³⁹ *Zubulake v. UBS Warburg* (“*Zubulake I*”), 217 F.R.D. 309, 321-322 (S.D. N.Y. 2003).

⁴⁰ *Id.* at 318.

⁴¹ We have modified the fifth *Zubulake I* category by splitting the concept into “Physically damaged media” and “Legacy media.” Physically damaged media involves media that cannot be read without forensic assistance or specialized software tools and Legacy media involves orphaned media where it is difficult to locate a compatible drive or device to read the typically old or legacy media.

⁴² That the data is deemed “accessible” does not mean it is readily available, “the time it takes to actually access [such] data ranges from milliseconds to days, [however] the data does not need to be restored or otherwise manipulated to be usable”. Inaccessible data, on

B. Data Complexity Factors

The Sedona Conference® also believes, however, that consideration must be given to the unique complexities of retrieval and review of data from any given source, depending upon the nature of the burdens involved. Accordingly, we have suggested six *additional* Sedona Accessibility Factors (See Figure 2) that should be considered along with the media based factors in reaching an overall measure of the relative inaccessibility of the data source.

For example, claim forms which are scanned to an active on-line server storage device in a "TIF" graphics format that does not allow for text search are "Active on-line data," but because the Search Complexity (Factor 11) is high and manual review is expensive, a more nuanced and complete view is that the source of those claim forms is relatively inaccessible for purposes of analysis.

Thus, we recommend that the user address *both* the media and data complexity factors under the facts and circumstances of the case before arriving at a relative accessibility rating for purposes of the Decision Tree.

The quality of the documentation related to the "not reasonably accessible decisions" will be of importance in discovery related motions and assist the court in determining whether a party acted reasonably, even if mistakenly, under the facts and circumstances of a given case.

the other hand, is not readily usable. Backup tapes must be restored ... fragmented data must be defragmented, and erased data must be reconstructed. That makes such data inaccessible." *Id.* at 318-321.

Figure 2
Accessibility Factors

	Factors	Examples
1	<i>Active on-line data</i>	Hard drives, PDAs, network storage
2	<i>Near-line data</i>	Robotic storage devices such as optical disks
3	<i>Offline storage/archives</i>	Removable optical disks or magnetic tape media which can be labeled and stored in a shelf or rack
4	<i>Backup tapes</i>	Sequential access devices typically not organized for retrieval of individual documents or files
5	<i>Physically damaged media</i>	Damaged CDs or DVDs that cannot be read by an ordinary drive or damaged hard drives and tapes
6	<i>Legacy media</i>	Difficult or impossible to locate a compatible drive or device to read the typically “orphaned” legacy media
7	<i>Transient complexity</i>	Web pages constantly being deleted and overwritten to make room for further storage
8	<i>Hidden complexity</i>	Deleted files after recycle bin has been emptied which cannot be viewed without specialized knowledge or tools
9	<i>Extraction complexity</i>	Data fragments found in the slack space which are difficult to copy
10	<i>Preservation complexity</i>	Cache and temp files created by a PC difficult to preserve without disabling operating system
11	<i>Search complexity</i>	Static graphical images not OCR’d
12	<i>Dispersion complexity</i>	Numbers of PDA devices needed to be reviewed for preservation of data from a central synchronized location

Step Four Analysis – Availability of Alternative Sources

When assessing the need to preserve inaccessible sources, an important factor is whether the identical or substantially similar information is available through more accessible sources.

In most instances, it is reasonable to rely upon the existence of alternative sources of the same or substantially similar information as a reason for not preserving a particular source of the same information. This is true whether the source in question is itself reasonably accessible (in which case the information is essentially duplicative) or may be deemed to be inaccessible (in which case it is not only duplicative, but more onerous to retrieve and utilize). The Committee Note to Rule 37(e) suggests that whether affirmative action is required often depends on “whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources.”

Illustration i. In a dispute over the termination of an employee, the active email accounts of key players are captured as soon as a producing party reasonably anticipates litigation, and the question is raised as to whether it is necessary to set aside existing backup media for the email servers, which are routinely overwritten. One of the factors to consider is whether deleted information will not be found in the active accounts and is therefore available only on one or more of the existing backup media.

Illustration ii. Under the same set of facts as above, the issue is whether it is necessary to make a mirror image or otherwise preserve the hard drive from the workstation or from the laptop used by the former supervisor of the terminated individual who has left the company for unrelated reasons.

The resolution of the issue often turns on the reasonableness of the belief of the party responsible for the source at issue. The burden of proof on the issue may vary with the circumstances. In *Cache La Poudre Feeds v. Land O’Lakes*,⁴³ the court sanctioned the failure to retain the hard drives of key former employees while questioning the basis for the General Counsel’s belief that the relevant information could be found in a more readily accessible location, given that the General Counsel was aware that email backup tapes were not being retained, but were being recycled. In *Best Buy Stores v. Developers Diversified Realty*,⁴⁴ however, no sanctions issued because the party questioning the failure to act did not argue and prove that database materials were uniquely available from the inaccessible source.⁴⁵

In *Disability Rights Council v. WMTA*,⁴⁶ the Magistrate Judge noted a failure (which the court described as “indefensible”) to prevent the automatic deletion of email, including “possibly relevant and discoverable emails.”⁴⁷ As recently noted by two well-regarded e-discovery thought leaders,⁴⁸ “[a] party cannot be acting in good faith unless it takes some steps to preserve information once litigation is reasonably anticipated.”

One of the more subtle issues involves the degree of responsibility of a party whose employees disregard otherwise reasonable legal hold or litigation hold instructions. In *Hawaiian Airlines, Inc. v. Mesa Air Group*,⁴⁹ for example, a court entered an adverse inference instruction against a party that could have, but did not, make backups of the hard drives of a key executive immediately after suit was filed. The court found that the employer had a duty to act

⁴³ 2007 WL 684001 (D. Colo. March 2, 2007).

⁴⁴ 247 F.R.D. 567 (D. Minn. November 29, 2007) (reversing Magistrate Judge opinion and noting that any relevant ESI could be gathered manually without the need for restoration of the database).

⁴⁵ *Id.* at 571.

⁴⁶ 242 F.R.D. 139 (D.D.C. June 1, 2007).

⁴⁷ *Id.* at *146 (noting that users may defeat the automatic deletion by archiving the email, which a majority of employees did not do).

⁴⁸ See Shira A. Scheindlin and Jonathan M. Redgrave, “E-Discovery: Technology Requires Greater Care in Preserving Evidence,” April 2008 ABA Journal, at p. 53.

⁴⁹ 2007 WL 3172642 (Bkrcty. D. Ha. Oct. 30, 2007) (CFO intentionally scrubbed files from laptop computers after receiving legal hold notice).

given the risk that high level employees might do “wrongful and foolish things, like destroying evidence, under the pressure of litigation.” The reasonableness of reliance on employees to follow directions must be assessed in the context of the particular facts and circumstances.

Step Five Analysis – the Proportionality Principle

If the burdens and costs of preservation are disproportionate to the potential value of the source of data at issue, it is reasonable to decline to preserve the source.

The concept of proportionality pervades discovery obligations resting on the Federal Rules of Civil Procedure. Rule 1 highlights the imperative that all of the procedural rules, including the discovery rules, “be construed and administered to secure the just, speedy, and inexpensive determination of every action and proceeding.” Proportionality underlies the concept in Rule 26(b)(2)(B) that data sources can include those which are “not reasonably accessible because of undue burden or cost.” And Rule 26(b)(2)(C) of the Federal Rules provides, in part, that the ability to conduct discovery must be limited to those instances where the anticipated benefits outweigh the burdens and costs of the discovery.

These considerations of proportionality are intended to balance the costs and potential benefits of discovery and are applicable, by way of analogy, to implementation of the duty to preserve.⁵⁰ As noted in Comment 2.b of *The Sedona Principles*, “[o]therwise, transactional costs due to electronic discovery will overwhelm the ability to resolve disputes fairly in litigation.”

It is the proportionality principle that reconciles, under the Decision Tree analysis, the widely varying circumstances under which a party - in the absence of agreement - must make its decisions independent of the technical characteristics of the data source. For example, an employee’s local drive may not warrant forensic imaging in a straightforward commercial dispute, whereas it could be crucial to (and thus need to be preserved) in a trade secret case.

In weighing proportionality, the burdens and costs of accessing and preserving the information on the source, as already identified in Step Three, are balanced against the reasonably anticipated need and significance of the information in the imminent or pending cases. If such costs and burdens do not outweigh the reasonably anticipated importance in that context, preservation is warranted. Conversely, if the burdens and cost of preservation is disproportionate to the reasonably anticipated value, preservation would not be required.

Illustration. In a dispute where potentially discoverable information is stored on a cell phone SIM file, the data source is assessed as relatively inaccessible. Given this determination, the issue then becomes, under Step Four of the Decision Tree, whether the information sought is uniquely available on the SIM card. If so, the ultimate issue, as posed by Step Five, is whether the perceived benefit to ultimate discovery is outweighed by the burdens and costs of the preservation of the information.

The duty to preserve does not require a disproportionate investment in hardware or software to effectuate such preservation. For example, in *Proctor & Gamble Company v. Haugen*,⁵¹ the Court of Appeals reversed an order of sanctions because the preservation steps not taken would have required installation of a new server or the purchase of archival data from a third party.⁵² Similarly, in *Malletier v. Dooney & Bourke, Inc.*,⁵³ an entity maintaining a chat room function for its customers was not required to activate or install a method of recording the comments.

⁵⁰ See *Oxford House v. City of Topeka, Kansas*, 2007 WL 1246200 (D. Kan. April 27, 2007) (no duty to maintain email or recover from backup media given that cost was not justified by low probability that information would be recovered).

⁵¹ 427 F.3d 727 (10th Cir. 2005).

⁵² *Id.* at 739.

⁵³ 2006 WL 3851151 (S.D.N.Y. Dec. 22, 2006).

Similarly, a party is not required to create information that does not exist. In *Getty Properties Corp. v. Raceway Petroleum*,⁵⁴ the Court denied an adverse inference for a failure to “create and preserve” alarm history reports prior to being ordered to do so because the failure to “create more reports than it used in the daily activities of its business is not the kind of willful action that discovery sanctions are intended to redress.” Similarly, in *Phillips v. Netblue*,⁵⁵ the failure to preserve URLs to advertisements or to memorialize hyperlinks images was not sanctioned because “[t]his is not a complaint regarding [an] alleged failure to preserve evidence, but rather [an] alleged failure to gather evidence.”⁵⁶ (Emphasis in original.)

Finally, the principle of proportionality also plays an important role in deciding whether specific metadata should be preserved. It is often advisable to preserve sources of electronically stored information in native file formats with metadata if there is a possibility that production will be subsequently sought in that form.⁵⁷ Comment 12.b of *The Sedona Principles*⁵⁸ suggests that organizations “evaluate the potential benefits of retaining native files and metadata (whether or not it is produced) to ensure that documents are authentic and to preclude the fraudulent creation of evidence.”

However, if the necessity to do so is not obvious, the burdens associated with any enhanced privilege review and the possibility that the metadata will not be needed for production purposes may be taken into account in deciding whether or not to preserve. For example, cases involving patent, unfair competition, trademark, and antitrust often raise disproportionate review concerns because the metadata may include privileged material and thus require extensive review.⁵⁹

Guideline 2. *As soon as feasible, preservation issues should be openly and cooperatively discussed in sufficient detail so the parties can reach mutually satisfactory accommodation and also evaluate the need, if any, to seek court intervention or assistance.*

Rule 26(f) lists “issues” relating to preservation as among the key topics for discussion prior to development of Scheduling Orders under Rule 16(b). This paradigm shift contemplates greater transparency about preservation issues and also implies, as its necessary corollary, that waiver of subsequent spoliation claims may result where parties do not take advantage of the opportunities to discuss the issues.

Accordingly, the parties should discuss issues relevant to preservation in sufficient detail to adequately explore the possibility of reaching agreement on practical methods of resolving contentious issues. This includes, for example, the anticipated form or form of production and the related need for metadata and native format so that the matter can be resolved while the information is still in native format. This preserves the ability of the producing party to prepare an appropriate extract of any metadata that may be required or to make production in some variant of a native file format.

⁵⁴ 2005 WL 1412134 (D.N.J. June 14, 2005).

⁵⁵ 2007 WL 174459 (N.D. Cal. Jan. 22, 2007).

⁵⁶ This holding may be inconsistent with *Columbia Pictures v. Bunnell*, *supra*, 2007 WL 2080419 (C.D. May 29, 2007)(Magistrate Judge Chooljian); *aff'd*, 245 F.R.D. 443 (C.D. Cal. Aug. 24, 2007), where the Magistrate Judge ordered a party to begin to preserve temporary information which could be logged without undue burden. See Thomas Y. Allman and Kevin Brady, *Can Random Access Make Good Law?* The National Law Journal, Vol. 30, No. 15 (December 10, 2007) (noting that *National Union Electric v. Matsushita* (1980), held that “common sense” required production in machine-readable format despite the fact that the information did not exist in that precise form).

⁵⁷ See *United States v. O'Keefe* Cr. No. 06-249 (PLF/JMF), 2008 WL 449729 (D.D.C. Feb. 18, 2008) (applying amended Rule 34(b) as persuasive authority in the criminal discovery context to require the government to preserve electronically stored information in its native format with metadata until the motion regarding production ruled upon).

⁵⁸ See *The Sedona Principles* (2nd ed. 2007, www.thesedonaconference.org), Principle 12 (decisions should take 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).

⁵⁹ See Jack E. Pace, III & John D. Rue, *Early Reflections on E-Discovery in Antitrust Litigation: Ten Months Into the New Regime*, 22 ANTITRUST 67, 69 (2007) (“[T]he costs associated with just the additional privilege review that would be necessary for each and every production of ESI (including metadata) could be staggering.”).

A number of practical examples exist. For example, in *In re Celexa and Lexapro Products Liability Litigation*,⁶⁰ the parties agreed that the producing party could set aside for future consideration a selection of existing backup media while resuming recycling of the remainder. Further, in the case of *In re Genetically Modified Rice Litigation*,⁶¹ the agreed order required the parties to take reasonable steps to preserve defined information from active files in native format pending discovery.

Illustration. The class representative in a complex pharmaceutical class action seeking discoverable information from a multitude of databases is informed that they are not programmed to isolate and produce information regarding the issues in the case. After consultation, an agreed process is established whereby the parties will identify experts to discuss the best technical means of preserving the information pending the discovery phase.⁶²

In preservation discussions, parties “should pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities. Complete or broad cessation of a party’s routine computer operations could paralyze the party’s activities.”⁶³ However, willful continuance of a routine operation involving destruction when preservation obligations are known to apply is not an example of “good faith” operation of that system.

Where parties are unable to reach agreement, either or both should consider whether to seek court resolution of preservation issues involving inaccessible sources. Although the Advisory Committee discouraged *ex parte* or unreasonably broad preservation orders,⁶⁴ it also acknowledged the practical benefits of preservation orders and clearly contemplated that courts would and should entertain them, where appropriate. In some cases, it may also be appropriate to allocate the costs of preservation if the marginal value is minimal.⁶⁵

Guideline 3. *In conjunction with the initial discussions or where appropriate in the response to discovery requests, parties should clearly identify the inaccessible sources reasonably related to the discovery or claims which are not being searched or preserved.*

Rule 26(b)(2)(B) requires that a party “identify” any inaccessible sources it does not intend to search in order to qualify for the presumptive limitation on the need to search. However, the Rule and the Committee Note do not dictate when or how that identification must be made.

There are several opportunities to make the necessary identification of such sources.

A. Initial Disclosure (Rule 26(a)(1))

Rule 26(a)(1) requires a listing of inaccessible sources not being searched only if there is a credible possibility that they may contain information that a party “may use to support its claims or defenses.”

⁶⁰ 2006 WL 3497757 (E.D. Miss. Nov. 13, 2006). See also Friedberg, “To Recycle or Not to Recycle, That is the Hot Backup Tape Question,” 201 PLI/Crim. 205, 217 (2005) (recommending alternatives to avoid suspension of email backup rotation).

⁶¹ 2007 WL 1655757 (E.D. Mo. June 5, 2007).

⁶² See *In re Seroquel Products Liability Litigation*, 2007 WL 219989, at *4 (M.D. Fla. Jan. 26, 2007). That this effort is no small task can be seen from *In re Seroquel Products Liability Litigation*, 2007 WL 2412946, at *12 (M.D. Fla. Aug. 21, 2007) (criticizing the “purposeful sluggishness” of defendant in carrying out obligations under the agreed order).

⁶³ Committee Note, Rule 26(f).

⁶⁴ *Id.* (“The requirement that the parties discuss preservation does not imply that courts should routinely enter preservation orders. A preservation order entered over objections should be narrowly tailored. Ex parte preservation orders should issue only in exceptional circumstances.”).

⁶⁵ See *Treppel v. Biovail Corp* (S.D.N.Y. 2006) (“If the demanding party seeks the preservation of information that is likely to be of only marginal relevance but is costly to retain, then rather than deny a preservation order altogether, a court may condition it upon the requesting party assuming responsibility for part or all of the expense.”).

B. Meet and Confer

The Committee Note to Rule 26(f) suggests that parties discuss whether the information that may be sought in discovery is reasonably accessible. This should be accomplished in sufficient detail so that the requesting party can make its own determination as to whether it wishes to seek production from any inaccessible sources not being searched. Some local rules make this discussion mandatory at or prior to the “meet and confer.”⁶⁶

A list of possible topics for discussion include:

- Type of back-up and disaster recovery media used.
- Identity and version of legacy software or systems, and when such software or systems achieved “legacy” status within an organization.
- Information sufficient to describe the system(s) or protocols used by the party to map, archive, and manage the back-up processes and procedures.
- Information describing sources of information that are or may be duplicative or substantially similar to the information sought – and the processes used to locate those sources.
- Internal or third-party estimates of costs associated with accessing the various sources of data involved.
- Detail about the capture and retrieval protocol under consideration, and the internal cost of data capture and retrieval (human capital of an organization to restore or extract data).
- “Extenuating circumstances,” including any potential opportunity-cost issues associated with allocating internal staff to restore or extract data (e.g., an organization relying on a new product roll-out for survival).
- The anticipated form or forms of production to be sought, the need for metadata, and the form of preservation of information pending discovery.

Parties may also wish to document their discussion of factors supporting their claim of inaccessibility. The documentation should include, if feasible, any costs or other burdens created by such preservation.

C. Objections to requests for production

A party seeking discovery under Rule 34(a) must set forth, by individual item or by category, the items sought with “reasonable particularity.” A written response must be made stating compliance or, if the request is objected to, the “reasons for the objection.”

The potential sources of discoverable information that are not being searched should be clearly identified in any response, in a manner analogous to traditional objections, if this has not already been adequately conveyed at the meet and confer or otherwise. Formal objections may also include the information sufficient to accomplish the identification.

⁶⁶ See “Guidelines for Discovery of Electronically Stored Information,” District of Kansas, Para. 4(g), available at <http://www.ksduscourts.gov/guidelines/electronicdiscoveryguidelines.pdf> (“If the responding party is not searching or does not plan to search sources containing potentially responsive information, it should identify the category or type of such information.”). See also *Default Standard for Discovery Of Electronically Stored Information, Appendix K*, Northern District of Ohio (“Prior to the Rule 26(f) conference, the parties should [discuss] whether . . . electronically stored information is of limited accessibility [such as] those created or used by electronic media no longer in use, maintained in redundant electronic storage media, or for which retrieval involves substantial cost.”), available at http://www.ohnd.uscourts.gov/Clerk_s_Office/Local_Rules/AppendixK.pdf.

D. Form and Content of Identification

Rule 26(b)(2)(B) does not explicitly define what information must be furnished in any “identification,” thus leaving room for differing approaches. The Committee Note suggests that the party “identify, by category or type” the sources it is neither searching nor producing. The Committee Note also states, however, that the identification should “to the extent possible” provide enough detail to enable the requesting party to determine if it wishes to seek additional information or challenge the designation.

More than one round of discussions and supplemental disclosures may be necessary to provide adequate identification. The totality of the information provided should be the touchstone of compliance. There should be no single formula or mechanical requirement.

Guideline 4. *A party should exercise caution when it decides for business reasons to move potentially discoverable information subject to a preservation duty from accessible to less accessible data stores.*

A party may decide, for business reasons, to store potentially discoverable information subject to a preservation duty in any media it chooses provided that the information can still be produced in discovery.⁶⁷ In *Best Buy Stores v. Developers Div. Realty*,⁶⁸ for example, a court dealt with information that had been stored on backup media after an earlier litigation. The District Court, overruling a Magistrate Judge, refused to sanction the producing party, noting that the information remained available for discovery but could more likely be acquired directly.⁶⁹

In *Quinby v. WestLB AG*,⁷⁰ a court refused to sanction a party for moving email to backup media from active media, but did decline to shift the costs of restoring email from the inaccessible media, noting the conflicting view of another Magistrate Judge in *Treppel v. Biovail*.⁷¹ The court held that a party should be free to preserve electronic evidence in any format it chooses and cautioned that any other result would implicate “a whole range of document storage practices, such as off-site storage in ‘dead’ files,” and would “create the potential for punishing routine business practices that do not destroy documents or alter them in any material sense.”

Guideline 5. *It is acceptable practice, in the absence of an applicable preservation duty, for entities to manage their information in a way that minimizes accumulations of inaccessible data, provided that adequate provisions are made to accommodate preservation imperatives.*

All organizations necessarily employ some type of management, formal or not, of their organization to meet regulatory, legal, and business needs. When information in electronic form accumulates in data sources which are difficult to access, however, it can become impracticable to assess their content and thereby manage them in a compliant manner. Efforts to do so are complicated over time by changes and upgrades in technology. Mergers, acquisitions, and sales of blocks of business add organizational challenges to the already daunting technical issues involved in accommodating differing systems. This problem can be compounded when entities fail to adopt appropriate policies and procedures that are responsive to the issues.

Effective management of information - including information stored on inaccessible sources - is largely governed by business and regulatory considerations, and courts will defer to those decisions provided that no actions are undertaken which are intended to and do interfere with the access to the information for discovery purposes.⁷²

⁶⁷ See *Quinby v. WestLB AG*, 2005 WL 3453908 (S.D.N.Y. Dec. 15, 2005) (“*Quinby I*”).

⁶⁸ 247 F.R.D 567 (D. Minn. 2007).

⁶⁹ *Id.* at 571.

⁷⁰ 2006 WL 2597900 (S.D.N.Y. Sept. 5, 2006).

⁷¹ See *Treppel v. Biovail*, 223 F.R.D. 363, 372 (S.D.N.Y. 2006) (“conduct that hinders access to relevant information is sanctionable, even if it does not result in the loss or destruction of evidence”).

⁷² See *Arthur Anderson LLP v. United States*, 544 U.S. 696 (2005) (destruction of information pursuant to a “valid document retention policy” is not “wrongful” under “ordinary circumstances”). See *Stevenson v. Union Pacific Railroad Company*, 354 F.3d 739, 746 (8th Cir. 2004) (holding that “some indication of an intent to destroy the evidence for the purpose of obstructing or suppressing the truth” is required); but see *Residential Funding Corporation v. DeGeorge Financial Corp.*, 306 F.3d 99, 107-8 (2d Cir. 2002) (determining culpability by negligence standard). Compliant data management practices regarding information security are discussed in ISO 27002,

Federal law requires a variety of regulated entities to adopt policies and procedures to ensure the security of information, to protect against unauthorized access or use, and to destroy the information through special, secure methods.⁷³ Absent regulations and specific preservation obligations, public and private organizations and individuals are empowered to minimize the volume of inaccessible data retained. The following are examples of ordinary course of business practices that could be considered:

- Overwriting residual data on hard drives.
- Overwriting or destroying used hard drives prior to repurpose or disposal of workstations or other hardware devices.
- Removing some metadata from documents in retaining them as records or when transmitting them to others.⁷⁴
- Restricting the capture of back-up data to the purpose of disaster recovery restoration, rather than archival data storage, and limiting the life of back-up data to the minimum time period necessary to fulfill the purpose of disaster recovery.
- Identifying inaccessible data sources containing legacy data; using reasonable efforts to assess whether the sources contain data subject to retention obligations or preservation duties; and in the absence of a reasonable basis to conclude that retention obligations or preservation duties apply, compliantly disposing of such legacy data sources.

These practices also help reduce the information security risks associated with inaccessible data held in common nesting places such as back-up tapes, workstations, and other portable data storage devices, information sources that foreseeably will leave the entity's facilities in normal use or through hardware repurposing or retirement.

Guideline 6. *An entity should encourage appropriate cooperation among legal and other functions and business units within the organization to help ensure that preservation obligations are met and that resources are effectively utilized.*

Many organizations assign the lead coordination role for e-discovery response to their Legal Department, which collaborates with IT, compliance, and records management departments or functions. Other organizations prefer to create multi-disciplinary teams representing those departments or functions and others.

In any case, the task is to avoid or minimize miscommunications that can occur between Legal and IT, both in imposing and monitoring holds and preparing for discussions with opposing counsel. Counsel need to more actively and effectively participate in the e-discovery process. Both internal and retained counsel⁷⁵ should be

which “establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.” ISO 27002.1.

⁷³ See, e.g., 8 C.F.R. §274a.2(g) (entities retaining employee I-9 records in digital format); 12 C.F.R. part 30 Appendix B (credit unions and other financial institutions); 16 C.F.R. §314.3 (Gramm-Leach-Bliley regulated financial institutions); 17 C.F.R. §248.30(a) (SEC registered brokers, dealers, investment companies and investment advisors); 29 C.F.R. §1904.29(b)(6) (employers maintaining privacy case information related to OSHA 300 logs and OSHA 301 Incident Reports); 45 C.F.R. §164.306 (HIPAA covered entities); 16 C.F.R. §682 (requiring secure destruction of consumer report information). The great majority of states' privacy laws go further, imposing additional privacy protections not generally preempted by federal law and requiring entities to notify state residents of security breaches regarding their personal information.

⁷⁴ To retain all metadata would effectively limit the prevention of tampering in many commonly used software programs. For example, common technology that protects documents against tampering, such as the “pdf” format or the Write-Once-Read-Many technology used in many email archives, does not capture all of the transactional or embedded metadata in word processing documents, e-mail, or other e-communications.

⁷⁵ The ABA Discovery Standards distinguish between the preservation obligations of a party and the responsibilities of its counsel. See ABA CIV. DISCOVERY STANDARDS (1999), as amended (August 2004) (limiting, in Standard 10, counsel responsibilities to those involving advice regarding preservation and consequences of failures). Compare *Zubulake v. UBS Warburg*, 229 F.R.D. 422, 435 (S.D. N.Y. 2004) (“*Zubulake V*”) (“counsel [both employed counsel and outside counsel] [are] responsible for coordinating her client’s

concerned about the degree to which a party meets its obligations to preserve inaccessible information. In *Phoenix Four, Inc. v. Strategic Resources Corporation*,⁷⁶ the court sanctioned a party and its law firm for failure to locate inaccessible information because it did not conduct a “methodical survey of [Defendants] sources of information” in the manner said to be required by the 2006 Amendments.

The Committee Note to Rule 26(f) suggests that counsel should become “familiar” with a client’s information systems to a sufficient degree necessary to permit discussion of potential issues that may be involved.⁷⁷ Local District Rules⁷⁸ and electronic discovery “guidelines”⁷⁹ often reinforce this expectation and in some cases mandate a degree of preparation beyond that implied by the Committee Note.⁸⁰

Consideration should also be given to implementing enhanced technology to improve internal processes. A diligent and cooperative effort with the IT functions of entities may yield opportunities for relatively cost-effective investments that will assist in managing inaccessible information.

The outsourcing of IT and document management functions and of less accessible information stores by many organizations imposes a need to be able to rely on the abilities of third parties to implement the hold procedures of their customer organizations when the third parties maintain ESI within their customers’ control.⁸¹ These obligations should be addressed specifically at the commencement of the relationship, and vendor management participation in preservation teams and processes can be important.

The degree to which a party must or should employ recently developed technology or revised business practices should be justified by business considerations. Information Management-related risks are recognized as a significant component of business risk,⁸² and many business expenditures on information technology can be leveraged for business and compliance purposes. Some organizations treat needs for compliant preservation activities as just one dimension of their needs to gain greater control over their information assets and sensitive data.

The business case for improvements in advanced search and storage options will necessarily continue to evolve. As recent and future technology substantially lessens the burdens and costs of locating relevant ESI on back-up media or in other less accessible information stores, technology to make archival systems more accessible and searchable also improves. Therefore, the periodic destruction of back-up media not needed for the disaster recovery purposes for which they were designed, and the reliance for archival and preservation purposes on more accessible and searchable media designed for those purposes, is likely to remain good practice.

discovery efforts. In this case counsel failed to properly oversee UBS in a number of important ways, both in terms of its duty to locate relevant information and its duty to preserve and timely produce that information”).

⁷⁶ 2006 WL 1409413 (S.D. N.Y. May 23, 2006).

⁷⁷ A failure to acquire sufficient knowledge to engage in such discussions arguably violates the ethical obligation to provide competent representation. See ABA MODEL RULES OF PROF’L CONDUCT R. 1.1 (2002) (“legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation”). Compare *Thompson v. Jiffy Lube Int’l*, No. 05-1203-WEB, 2006 WL 3388502, at *2 (D. Kan. Nov. 21, 2006) (failure to take action regarding order relating to email system “raises serious questions about counsel’s experience, knowledge of applicable law, and resources available [to represent class]”).

⁷⁸ See, e.g., E.D. & W.D. ARK. LOC. R. 26.1; D. DEL.R. 16(4)(B); D.N.J. LOC. CIV. R. 26.1; D. WYO. LOC. R. 26.1.

⁷⁹ See “Guidelines for Discovery of Electronically Stored Information,” District of Kansas, ¶1, (Oct. 2006), available at <http://www.ksd.uscourts.gov/guidelines/electronicdiscoveryguidelines.pdf>.

⁸⁰ See *Id.* at ¶ 2 (requiring disclosure of “individuals with knowledge of their client’s electronic systems” prior to the conference). See Steven C. Bennett, *The Ethics of Electronic Discovery*, Vol. 17 No. 2 PRAC. LITIGATOR 45, 48 (Mar. 2006) (emphasizing the obligation to provide “competent” representation).

⁸¹ See *Tomlinson v. El Paso Corp.*, 2007 WL 2521806 (D.Colo. Aug. 31, 2007)(production of ERISA data maintained by third party must be produced as within custody and control).

⁸² Richard Hunter, *IT Risk: Turning Business Threats into Competitive Advantage*, Harvard Business School Press, 2007.

Appendix A: The Sedona Conference[®] Working Group SeriesSM & WGSSM Membership Program

**“DIALOGUE
DESIGNED
TO MOVE
THE LAW
FORWARD
IN A
REASONED
AND JUST
WAY”**

The Sedona Conference[®] Working Group SeriesSM (“WGSSM”) represents the evolution of The Sedona Conference[®] from a forum for advanced dialogue to an open think-tank confronting some of the most challenging issues faced by our legal system today.

The WGSSM begins with the same high caliber of participants as our regular season conferences. The total, active group, however, is limited to 30-35 instead of 60. Further, in lieu of finished papers being posted on the website in advance of the Conference, thought pieces and other ideas are exchanged ahead of time, and the Working Group meeting becomes the opportunity to create a set of recommendations, guidelines or other position piece designed to be of immediate benefit to the bench and bar, and to move the law forward in a reasoned and just way. Working Group output, when complete, is then put through a peer review process, including where possible critique at one of our regular season conferences, hopefully resulting in authoritative, meaningful and balanced final papers for publication and distribution.

The first Working Group was convened in October 2002, and was dedicated to the development of guidelines for electronic document retention and production. The impact of its first (draft) publication—The Sedona Principles; Best Practices Recommendations and Principles Addressing Electronic Document Production (March 2003 version)—was immediate and substantial. The Principles was cited in the Judicial Conference of the United State Advisory Committee on Civil Rules Discovery Subcommittee Report on Electronic Discovery less than a month after the publication of the “public comment” draft, and was cited in a seminal e-discovery decision of the Federal District Court in New York less than a month after that. As noted in the June 2003 issue of Pike & Fischer’s Digital Discovery and E-Evidence, “The Principles...influence is already becoming evident.”

The WGSSM Membership Program was established to provide a vehicle to allow any interested jurist, attorney, academic or consultant to participate in Working Group activities. Membership provides access to advance drafts of Working Group output with the opportunity for early input, and to a Bulletin Board where reference materials are posted and current news and other matters of interest can be discussed. Members may also indicate their willingness to volunteer for special Project Team assignment, and a Member’s Roster is included in Working Group publications.

We currently have active Working Groups in the areas of 1) electronic document retention and production; 2) protective orders, confidentiality, and public access; 3) the role of economics in antitrust; 4) the intersection of the patent and antitrust laws; (5) Markman hearings and claim construction; (6) international e-information disclosure and management issues; and (7) e-discovery in Canadian civil litigation. See the “Working Group Series” area of our website www.thesedonaconference.org for further details on our Working Group Series and the Membership Program.