Managing Discovery of Electronic Information: A Pocket Guide for Judges

Second Edition

Barbara J. Rothstein, Ronald J. Hedges, and
Elizabeth C. Wiggins

Federal Judicial Center
2012

This page is left blank intentionally to facilitate printing of this document double-sided.

Contents

This page is left blank intentionally to facilitate printing of this document double-sided.

Preface and introduction to the second edition

This second edition of the pocket guide on the discovery of electronically stored information (ESI) follows the first—and the related 2006 amendments to the Federal Rules—by more than five years. These intervening years have seen an explosion of civil case law on ESI. This case law interprets the 2006 amendments and sets forth practices that have proved helpful to the courts, lawyers, and litigants in the discovery and evidentiary use of ESI. In addition, with the adoption of Federal Rule of Evidence 502 in September 2008, the federal courts now have a common framework for analyzing privilege waiver issues and an effective way to reduce costs and delays that result from exhaustive preproduction review driven by a fear of wavier through inadvertent disclosure.

Electronic information is ubiquitous. Information about our private and public lives, and information on the activities of all private and public entities are increasingly intermingled, interconnected, and stored on electronic media. The phrase "electronic media" has itself expanded to include various devices on which electronic information is created and stored, such as personal digital assistants (PDAs) and "smart phones," and the number and kinds of devices continue to grow and change. This expansion and the continuing changes in information technology have increased the complexities and costs of ESI discovery. As those complexities and costs grow, so does the need for effective discovery management. Judges must ensure that ESI discovery is planned properly, managed effectively, and supervised closely to avoid disputes, reduce costs and delays, and focus the case on the merits.

This pocket guide has been reorganized into a question and answer format, which we hope judges will find useful in meeting the challenges presented by the discovery of ESI. Its fundamental messages, however, are unchanged: Judges should actively manage cases that involve ESI through early intervention and sustained supervision. Judges should raise issues for the parties to consider rather than wait for the issues to be presented as full-blown disputes. They should use the many tools available to them—case-management conferences and orders, limits on discovery, tiered or phased discovery, sampling, cost shifting, and, if necessary, sanctions—to encourage cooperation

among opposing lawyers and to ensure that discovery is fair, reasonable, and proportional to each case. The particulars of case management, of course, depend on the extent the parties expect to rely on ESI in proving and defending their positions, the complexity of how ESI is created and stored, and other factors.

A note of appreciation goes to Judge Lee H. Rosenthal (S.D. Tex.), Ken Withers (The Sedona Conference), and John Rabiej (Center for Judicial Studies, Duke Law School) for their help in producing the first and second editions. In addition, Mukai S. Amoo, William P. Butterfield, Maura R. Grossman, Sherry B. Harris, Emery Lee, and Jeane A. Thomas provided valuable suggestions that improved this guide.

What is electronically stored information (ESI) and how does it differ from conventional paper-based information?

ESI currently includes e-mail messages, word processing files, web pages, and databases created and stored on computers, magnetic disks (such as computer hard drives), optical disks (such as DVDs and CDs), and flash memory (such as "thumb" or "flash" drives), and increasingly on "cloud" based servers hosted by third parties that are accessed through Internet connections. The technology changes rapidly, making a complete list impossible. Federal Rules of Civil Procedure 26 and 34, which went into effect on December 1, 2006, use the broad term "electronically stored information" to identify a distinct category of information that, along with "documents" and "things," is subject to discovery rights and obligations.

ESI differs from conventional, paper-based information in several ways that affect discovery. The volume of ESI is almost always exponentially greater than that of paper information, and ESI may be located in multiple places that are widely dispersed. For example, draft and final versions of a single memorandum may be stored electronically in multiple places (e.g., on the computer hard drives of the document's creator, reviewers, and recipients; on the company server; on laptops and home computers; on backup tapes; and on local network servers and third-party hosted servers). Market research has found that the average employee sends or receives more than 100 electronic messages per working day, which translates into more than 2,400,000 messages a year for an organization of 100 employees.

Although the possibility that paper documents or things could be damaged, altered, or destroyed has always been a concern, the dynamic and mutable nature of ESI presents new challenges. Computer systems automatically recycle and reuse memory space, altering potentially relevant information without any specific direction from, or even the knowledge of, the user. Merely opening a digital file changes information about that file, and e-mail messages may be automatically deleted after a certain period unless steps are taken to avoid it.

Some aspects of ESI have no counterpart in print media, metadata being the most obvious example.[1] Metadata, which most computer users never see, provide information about an electronic file, such as the date it was created, its author, when and by whom it was edited, what edits were made, and, in the case of e-mail, the history of its transmission. Another example is those computer-based transactions that do not result in printable text-based documents, but instead are represented in specially formatted databases. Even less complex ESI may be incomprehensible and unusable when separated from the system that created it. For example, financial projections developed using spreadsheet software may be useless if produced in portable document format (PDF) rather than in the format of the spreadsheet software because embedded information, such as computational formulas, is not retained in the PDF file.

How ESI differs from paper information

- Volume
- Variety of sources
- Dynamic quality and difficulty of preservation
- Hidden information: metadata and embedded data
- Varieties of forms for production
- Dependence on the system that created it
- Deleting doesn't necessarily delete it

Unlike paper documents, ESI can be produced in different forms, such as PDF and TIFF (tagged image file format). Some forms may not be compatible with the requesting party's computer system, may hide metadata and embedded data, and may not be as easy to search as the requesting party would like. If ESI was created on a system or with a program that is no longer used, either because it is obsolete or

1. See the terms *metadata*, *embedded data*, and *systems data* in the Glossary to this guide.

because the party does not have access to it, the information may be difficult to retrieve in a form that is useful.

Deleting an electronic document does not necessarily get rid of it, as throwing away or shredding a paper document would. An electronic document may be recovered from the hard drive or server, to the extent it has not been overwritten, and may be available on the computers of other people or on archival media or backup tapes used for disaster recovery purposes. The costs and efforts required to retrieve and restore such information, however, can be very high and extensive.

These and other differences between ESI and paper information have important implications for discovery. For example, the dynamic nature of ESI makes it vital that a litigant or potential litigant institute a "litigation hold" to preserve information that may be discoverable, whenever litigation is reasonably anticipated—and that can be well before a complaint is filed or an answer is served. The volume and multiple sources of ESI increase costs and burdens, which in turn leads to more disputes about whether discovery is relevant or proportional to the needs of the case. A review to identify and segregate privileged information is more difficult, increasing the likelihood of inadvertent production even when the producing party has taken reasonable steps to avoid it. Because deleted or backup information may be "relevant" under the discovery rules, parties may request its production, even though restoring, retrieving, and producing it may require expensive and burdensome computer forensic work that is disproportionate to the reasonable discovery needs of the requesting party. The choice of the form of production was not an issue with paper discovery, but it can lead to disputes in ESI discovery. Judges should be alert to the ways in which these differences may affect the discovery issues and management needs in their cases.

What is the judge's role in the discovery of ESI?

In the past decade, discovery involving word-processing documents, spreadsheets, e-mail, and other ESI has become common. Once seen primarily in large actions involving sophisticated entities, it is now seen in routine civil actions and increasingly in criminal actions. In many cases, ESI does not raise any issue. In some cases, ESI is con-

verted to paper and is exchanged in the traditional manner, although this sacrifices searchability and portability, and is therefore used less and less frequently. In most cases, ESI is produced and exchanged in electronic form.

In some cases, particularly cases that are complex or contentious, or in which the volume of ESI subject to discovery is large, disputes may arise. Some of these disputes will be difficult, time-consuming, and costly to resolve. Disputes may arise as to the scope of discovery of ESI. Disputes may arise over the form in which ESI is to be produced when one party finds that ESI has been delivered in a form that is not readily usable. Disputes may arise over whether inadvertent production of ESI waived attorney–client privilege or work-product protection. The producing party may seek to shift costs to the requesting party. One side may accuse the other of spoliation because routine file-management practices remained in place after the litigation was reasonably anticipated or the complaint was filed, and relevant computer files were deleted.

Judges can minimize such disputes by encouraging lawyers and parties to cooperate with one another and to identify, in the earliest stages of the litigation, potential problems in the discovery of ESI. The judge needs to work with the lawyers to ensure that planned discovery is reasonable and proportional to the needs of the case, and may need to intervene before misunderstandings lead to disputes and create significant cost and delay. When disputes do arise, it is often important to ensure that parties raise them quickly and that the judge decide them quickly, or the litigation will simply stop in its tracks. In short, discovery involving ESI may require more frequent and intensive judicial involvement than is required by conventional discovery.

In complex cases, these responsibilities are not easy undertakings. Like lawyers and litigants, judges have had to become familiar not only with the substantive issues of cases, but also with issues relating to how relevant electronic information is created and stored. Many district and magistrate judges have developed expertise in handling ESI discovery matters in recent years. If ESI issues are new to a judge or are complex, it may be useful for the judge to require parties to provide expert guidance on those issues. In some cases involving both high stakes and particularly contentious or difficult ESI discovery is-

sues, judges have found it appropriate to seek the assistance of a special master or neutral expert.[2]

How does a judge promote early consideration of ESI discovery issues?

Exchanging information in electronic form has significant benefits. It can substantially reduce copying, transport, and storage costs; enable the requesting party to more easily review, organize, and manage the information; facilitate the use of computerized litigation support systems; and set the stage for using ESI as evidence during pretrial and trial proceedings. To ensure that these benefits are achieved and any problems associated with ESI are minimized, judges should encourage attorneys and parties to address ESI in the earliest stages of litigation.

All too often, attorneys view their obligation to "meet and confer" under Rule 26(f) as a perfunctory exercise. When ESI is involved in a case, judges should insist that a meaningful Rule 26(f) conference take place and that a meaningful discovery plan be submitted for use in the Rule 16 conference with the court. In addition to specifying topics to be considered at the Rule 26(f) conference and included in the discovery plan to be submitted to the court, judges can make clear that the attorneys need to engage in advance preparation. Judges can also make clear that they expect the parties to establish a process for continuing discussion on ESI discovery issues, beyond a single Rule 26(f) conference. Judges can indicate to parties how to bring disputes before the court for efficient and prompt resolution. Any agreements the parties reach on how to protect against waiving attorney–client privilege or work-product protection by inadvertent production in discovery must be included in court orders to be effective as to third parties or in other cases (see related discussion *infra* pages 24–25).

2. For example, the judge may appoint a neutral expert to help develop a discovery plan and supervise technical aspects of discovery, review documents claimed to be privileged or protected, or participate in an on-site inspection. *See* Manual for Complex Litigation, Fourth § 11.446 (Federal Judicial Center 2004) [hereinafter MCL 4th] and The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production (The Sedona Conference Working Group Series June 2007) at comment 10.c, *available at* https://thesedonaconference.org/download-pub/81[hereinafter The Sedona Principles].

Therefore, the court should encourage parties to discuss this topic and to ask the court to include such agreements in Rule 16(b) orders.

Early in the case, the court should communicate its expectations as to how discovery will proceed. Case-management orders entered soon after a case is filed, standing orders, court guidelines and protocols, and local rules are all vehicles for doing so. Samples of such documents are available on the Federal Judicial Center's websites at http://cwn.fjc.dcn/fjconline/home.nsf/pages/196 and http://www.fjc.gov/public/home.nsf/pages/196.

What matters should be discussed at the Rule 26(f) conference?

Rule 26(f) directs parties to discuss any issues relating to disclosure or discovery of ESI, including the form or forms in which it should be produced. The specific issues that require attention during the Rule 26(f) conference depend on the specifics of the case and the extent and complexity of the contemplated discovery and ESI. To ensure that important matters are not overlooked, judges may want to provide a list of matters for the attorneys' consideration. Such lists can be found in existing local rules, protocols, and orders. Most such lists include the following:

- whether there will be discovery of ESI at all;
- disclosures required under Federal Rule of Civil Procedure 26(a)(1), if any, and their timing;
- what types or categories of discoverable information each party has in electronic form, and where and on what type of media that information is likely to be found;
- the steps each party will take to preserve different types or categories of ESI;[3]
- the number and identity of "key players" who are knowledgeable about potentially relevant ESI and on whose servers or devices ESI is likely to be found;
- what methods will be efficient in identifying discoverable ESI (e.g., sampling, key word searches);
- the anticipated schedule for production;

3. Specific discussion topics related to the preservation of information are listed in the MCL 4th, *supra* note 2, § 40.25(2).

- the form in which such information is ordinarily maintained and whether it will be produced in that form—usually known as "native format"—or in another form;
- the scope of discovery of different categories of ESI, such as e-mail messages;
- whether relevant information has been deleted, and if so, whether one or more parties believe deleted information needs to be restored and who will bear the cost of restoring it;
- whether any information is not "reasonably accessible," the burdens and costs of retrieving that information, why it is needed, and any conditions that should be placed on its production, including who will bear the cost; and
- whether relevant information is in the possession of nonparties from whom discovery under Rule 45 will be required.

Rule 26(f) also directs parties to discuss issues relating to procedures for asserting attorney–client privilege or work-product protection and for protecting against waiver. If parties agree on such procedures, they should discuss whether to ask the court to include their agreement in an order (see related discussion *infra* pages 24–25).

Discussion topics for a Rule 26(f) conference:

What ESI is available and where it resides

Preservation of information

Ease or difficulty and cost of producing information

Schedule of production

Form or forms of production

Agreements about attorney–client privilege or work-product protection

In preparation for the Rule 16 conference, parties should prepare a report describing points of agreement and matters in need of additional discussion or court intervention, and incorporate major points of agreement into a proposed order (see related discussion *infra* pages 11–12). If the parties disagree on any aspects of the discovery plan, they should prepare short statements of their respective positions for prompt resolution by the judge at the Rule 16 conference or shortly thereafter.

What preparations for the Rule 26(f) conference should be required?

For the Rule 26(f) conference to be effective, attorneys must be familiar with their clients' information systems. This familiarity usu-

ally requires understanding what information is available; how it may be altered or made unavailable by routine computer operations; and what is entailed in identifying, preserving, collecting, reviewing, and producing it. Attorneys need to identify those persons who are most knowledgeable about the client's computer systems and meet with them well in advance of the Rule 26(f) conference; it may also be useful to have those persons present at the conference. Some courts put such requirements in local rules, guidelines, or protocols; other courts use case-management orders to tell the attorneys what to expect.

For example, the District of Maryland's *Suggested Protocol for Discovery of Electronically Stored Information* provides detailed guidance to parties in preparing for the Rule 26(f) conference and anticipates that attorneys will

- discuss with their clients the facts underlying the litigation and advise their clients' information systems personnel of the substantive principles governing the preservation of relevant or discoverable ESI while the lawsuit is pending;
- become reasonably familiar with critical aspects of their clients' ESI or identify another person who is and can meaningfully participate in the Rule 26(f) conference;
- identify one or more information systems personnel to act as the ESI coordinator or coordinators and discuss ESI with them; and
- identify key persons in the lawsuit and determine their ESI practices.[4]

The District of Maryland and other districts also suggest or require that counsel exchange certain information before the Rule 26(f) conference. For example, the District of Delaware's *Default Standard for Discovery of Electronic Documents* requires the parties to exchange the following:

- a list of the most likely custodians of relevant electronic materials, including their titles and a brief description of their responsibilities;

4. U.S. District Court for the District of Maryland, Suggested Protocol for Discovery of Electronically Stored Information, http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf [hereinafter District of Maryland Protocol].

- a list of each relevant electronic system that has been in place at all relevant times and a general description of each system, including the nature, scope, character, and organization of the system and the formats it employs;
- other pertinent information about their electronic documents and whether those documents are of limited accessibility (e.g., they were created or used by electronic media no longer in use, they are maintained in redundant electronic storage media, or their retrieval would involve substantial cost);
- the name of the individual responsible for the party's electronic document retention policies, as well as a general description of the party's electronic document retention policies;
- the name of the person who will serve as the party's ESI discovery liaison, that is, the one individual who will receive and respond to all ESI discovery requests; and
- notice of any problems reasonably anticipated to arise in connection with ESI discovery.[5]

What continuing consultation between parties should be required?

In contentious or complex cases in which extensive discovery of ESI can be anticipated, the usual sequence of a Rule 26(f) conference, followed by the submission of a discovery plan and a Rule 16 conference with the judge may not be sufficient. In such cases, the judge may, upon request of the parties or sua sponte, require the parties to hold a series of conferences dealing with different aspects of discovery.

Rule 26(f) should be viewed as an ongoing *process* for negotiating a discovery plan that can prevent discovery disputes or identify them early so that they can be brought to the court for resolution before they become more complicated and difficult. The Rule 26(f) conference should not be viewed solely as a procedural ticket to be punched before formal discovery can begin.

---

5. Paraphrase of Ad Hoc Committee for Electronic Discovery of the U.S. District Court for the District of Delaware, Default Standard for Discovery of Electronic Documents ("E-Discovery"), http://www.ded.uscourts.gov/sites/default/files/Chambers/SLR/Misc/EDiscov.pdf [hereinafter District of Delaware Default Standard].

What matters should be covered during Rule 16 conferences and included in Rule 16(b) scheduling orders?

The Rule 16 conference with the judge and the resultant case-management and scheduling orders give the judge the best opportunity, early in the case, to work with the parties to ensure that ESI discovery is undertaken cooperatively and is reasonable and proportional to the needs of the case. The Rule 16 conference allows the judge to discuss and memorialize the agreements or shared understandings that parties have reached in their Rule 26(f) conference. The Rule 16 conference also allows the judge to identify any disputes and to resolve them early in the case. It is the judge's opportunity to work with the lawyers to craft a case-management order that is tailored to the case and that limits the scope of discovery to what is reasonably proportional to the needs of that case.

It is usually most helpful for the judge to hold "live" Rule 16 conferences with the attorneys present in court or in chambers. At a minimum, the judge should require the attorneys to participate by telephone or videoconference. Without the chance to talk with the attorneys, the judge may miss an important opportunity to uncover issues the attorneys have not identified or considered.

The court may require parties to come to the Rule 16 conference with a prepared Rule 26(f) report and a proposed scheduling order. Rule 16(b) provides that scheduling orders may include provisions for disclosure or discovery of ESI, and any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after production. Of course, the order will also include other key provisions, including the deadlines to join other parties, amend the pleadings, complete discovery, and file motions, and the dates for pretrial conferences and trial.

Some districts and judges facilitate this process by requiring that parties cover specified ESI matters in their Rule 26(f) reports. For example, Local Rule 26.1 for the Eastern and Western Districts of Arkansas specifies an outline for the report and requires that the report indicate whether any party is likely to be asked to disclose or produce ESI, and if so,

> (a) whether disclosure or production will be limited to data reasonably available to the parties in the ordinary course of business;

(b) the anticipated scope, cost, and time required for disclosure or production of data beyond what is reasonably available to the parties in the ordinary course of business;
(c) the format and media agreed to by the parties for the production of such data as well as agreed procedures for production;
(d) whether reasonable measures have been taken to preserve potentially discoverable data from alteration or destruction in the ordinary course of business or otherwise; and
(e) other problems which the parties anticipate may arise in connection with electronic or computer-based discovery.

Other courts specify that parties should indicate if they have entered into "clawback" or "quick peek" agreements, or agreed to testing or sampling provisions and, if so, the proposed treatment of ESI that is covered by attorney–client privilege or work-product protection, including what agreements they would like embodied in a court order.[6]

What disclosures of ESI are required under Rule 26(a)(1)?

Rule 26(a)(1) requires disclosure of the identities of individuals likely to have discoverable information, as well as "a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things" that the disclosing party may use to support its claims or defenses, unless they are to be used solely for impeachment. Initial disclosures must be made "at or within 14 days after the Rule 26(f) conference unless a different time is set by stipulation or court order."

Rule 26(a)(1) is not intended to require a party to undertake an exhaustive review of ESI in its possession, custody, or control. Instead, its purpose is "to enable opposing parties (1) to make an informed decision concerning which documents might need to be examined, at least initially, and (2) to frame their document requests in a manner likely to avoid squabbles resulting from the wording of the requests."[7] At a minimum, a party's initial disclosure should identify the nature of its computer systems, including its backup system, network system, and e-mail system and the software applications used by them.[8]

6. *See, e.g.,* District of Maryland Protocol, *supra* note 4, ¶ 4.
7. Fed. R. Civ. P. 26 advisory committee's note to 1993 Amendment.
8. *Compare* J. M. Moore, Moore's Federal Practice § 37A.20[2] (3d ed. 2010)

Except in the most straightforward cases, in which minimal discovery is anticipated or parties on both sides are familiar with the discovery that will be exchanged as a matter of routine practice, allowing parties to opt out of Rule 26(a)(1) disclosures can be problematic. If the parties want to opt out of Rule 26(a)(1) disclosures, they should present the court with a realistic alternative procedure for exchanging baseline information about the relevant information systems as necessary to plan ESI discovery, including key custodians of critical categories of ESI.

How does a judge limit the scope of ESI discovery to that proportional to the needs of the case?

The central issue in almost all discovery management is the determination of scope. Federal Rule of Civil Procedure 1 provides that the rules "should be construed and administered to secure the just, speedy, and inexpensive determination of every action and proceeding." As explained in the Advisory Committee note, the revision in 1993 to add the words "and administered" was intended to "recognize the affirmative duty of the court to exercise the authority conferred by these rules to ensure that civil litigation is resolved not only fairly, but also without undue cost or delay. As officers of the court, attorneys share this responsibility with the judge to whom the case is assigned." Rule 1 imposes an obligation on the bench and bar to take affirmative steps to ensure that discovery in any particular case is proportional to the stakes and issues involved in that case, and is undertaken with cooperation among parties.

Rule 26(b)(2)(C) requires that a judge limit discovery to what is proportional to the needs of the case. It provides that, on a party's motion or on its own initiative,

> the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that . . . the burden or expense of the proposed discovery outweighs its likely

---

(stating an exhaustive search of inaccessible sources is not required as part of the initial disclosure obligation) *with* United States District Court for the District of Kansas, Guidelines for Discovery of Electronically Stored Information (ESI), http://www.ksd.uscourts.gov/guidelines-for-esi/ [hereinafter District of Kansas Guidelines] (suggesting the search include "current back-up, archival, and legacy computer files").

> benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

Whether the proportionality requirement of Rule 26(b)(2)(C) is satisfied may depend on the type of ESI being sought. As with all information sought in discovery, ESI must be relevant to the claims or defenses asserted in the pleadings or, if good cause is shown, the subject matter of the dispute, and not privileged or protected. In the context of ESI, key custodians' production of active data, available to the responding party in the ordinary course of the party's activities, is most likely to satisfy the proportionality requirement. Active electronic records are generally those currently being created, received, or processed, or that need to be accessed frequently and quickly. Even requests for certain active ESI, however, may be disproportionate to the needs of the case. The Federal Circuit Advisory Council Model Order, for example, is premised on the idea that information obtained from mass e-mail searches is often tangential to the central issues in patent litigation.[9]

Systems data, which include such things as when people logged on and off a computer or network, the applications and passwords they used, and what websites they visited, may be more remote and more costly to produce. Other types of ESI are even more removed from what is available in the ordinary course of a party's activities, and their production may involve substantial costs and time and the active intervention of computer specialists. These types of ESI include offline archival media, backup tapes designed for restoring computer systems in the event of disaster, deleted files, and legacy data that were

9. The Advisory Council for the United States Court of Appeals for the Federal Circuit, An E-Discovery Model Order, http://www.cafc.uscourts.gov/the-court/advisory-council.html [hereinafter Federal Circuit Advisory Council Model Order]. In adopting its order, the Advisory Council noted that patent cases tend to suffer from disproportionately high discovery expenses, citing Emery G. Lee III & Thomas E. Willging, Litigation Costs in Civil Cases: Multivariate Analysis (Federal Judicial Center 2010). The order promotes the exchange of core documentation concerning the patent, the accused product, the prior act, and the finances before e-mail production requests are made. It requires e-mail production requests to be focused on a specific issue, and presumptively limits the number of custodians and search terms for such requests.

created on now-obsolete computer systems with obsolete operating and computer software.[10]

To ensure that the proportionality requirement is met, a judge may need to review the parties' proposed production requests. The judge should encourage the lawyers to stage the discovery by first searching for the ESI associated with the most critical or key players, examining the results of that search, and using those results to refine subsequent searches. The judge should make sure the lawyers are using search methods and criteria that are cost-effective and proportional to reasonable discovery needs.

When hard-to-access information is of potential interest, the judge should encourage or require lawyers to first sort through the information that can be obtained from easily accessed sources and then determine whether it is necessary to search the less accessible sources. The judge should also consider requiring parties to sample ESI that is not reasonably accessible to learn whether the benefits of a full search and of retrieving and restoring the ESI will justify the associated costs and burdens.

What type of information is "not reasonably accessible"?

A party asserting that ESI is "not reasonably accessible," and thus not subject to discovery under Rule 26(b)(2)(B) absent a showing of good cause, has the burden of proving the undue burdens and costs of accessing it.[11] A judge might require, among other things, an affidavit from a person with knowledge of the relevant systems, or from a qualified third party, detailing the procedures, anticipated costs, and foreseeable burdens of producing the ESI, presented in the context of the party's resources. A judge should not be content with generalized or conclusory statements about costs and burdens. Some courts have indicated that certain types of ESI are presumptively not reasonably

10. *See, e.g.,* Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 318–19 (S.D.N.Y. 2003) (describing the media on which ESI is maintained, and distinguishing active online data, near-line data, offline storage/archives, and backup tapes).

11. The Sedona Conference's Working Group 1 on Electronic Document Retention and Production proposes a set of six overarching principles for litigants and judges in considering the proportionality of discovery requests, particularly in the context of Rule 26(b)(2)(B). The Sedona Conference, *The Sedona Conference Commentary on Proportionality in Electronic Discovery*, 11 Sedona Conf. J. 289 (2010).

accessible. The Seventh Circuit Pilot Project Model Standing Order, for example, includes the following in that category:

(1) deleted, slack, fragmented, or unallocated data on hard drives;
(2) random access memory (RAM) or other ephemeral data;
(3) on-line access data such as temporary internet files, history, cache, cookies, etc.;
(4) data in metadata fields that are frequently updated automatically, such as last-opened dates;
(5) backup data that is substantially duplicative of data that is more accessible elsewhere; and
(6) other forms of ESI whose preservation requires extraordinary affirmative measures that are not utilized in the ordinary course of business.[12]

When does good cause exist to allow the discovery of "not reasonably accessible" information?

The requesting party may need discovery to challenge the assertion that the information is not reasonably accessible and to show good cause for the discovery to proceed. Such discovery may involve taking depositions of those knowledgeable about the responding party's information systems;[13] some form of inspection of the data sources; or requiring the responding party to conduct a sampling of information in the sources identified as not reasonably accessible. Sampling the less accessible sources can help refine the search parameters and determine the benefits and burdens associated with a fuller search.[14]

The Advisory Committee note to Rule 26(b)(2)(B) suggests that, in determining whether good cause exists to allow the discovery when the source of ESI is not reasonably accessible, the judge consider

---

12. Seventh Circuit Electronic Discovery Pilot Program, Principle 2.04(d) of the Seventh Circuit Pilot Project Model Standing Order, http://www.DiscoveryPilot.com/sites/default/files/StandingOrde8_10.pdf.

13. *See* Fed. R. Civ. P. 30(b)(6) (governing depositions directed at an organization). *See also* JSR Micro, Inc. v. QBE Ins. Corp., No. 09-03044, 2010 WL 1338152 (N.D. Cal. Apr. 5, 2010); 1100 West, LLC v. Red Spot Paint & Varnish Co., No. 05-1670, 2009 WL 1605118 (S.D. Ind. June 5, 2009).

14. The classic decision on sampling, which predates the 2006 amendments, is McPeek v. Ashcroft, 202 F.R.D. 31 (D.D.C. 2001). *See also* the subsequent decision, McPeek v. Ashcroft, 212 F.R.D. 33 (D.D.C. 2003).

(1) the specificity of the discovery request;
(2) the quantity of information available from other and more easily accessed sources;
(3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources;
(4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources;
(5) predictions as to the importance and usefulness of the further information;
(6) the importance of the issues at stake in the litigation; and
(7) the parties' resources.

In some cases, discovery of ESI from sources that are not reasonably accessible is unavoidable because of the claims and defenses. For example, the e-mail communications relevant to a disputed contract may have all occurred several years ago and are now only available from disaster recovery backup media. Or a claim of trade secret theft can only be established or defended by using system data showing access to the computer network at certain times. If the court permits the discovery of information from "not reasonably accessible" sources, the court may order that the requesting party pay all or part of the reasonable costs of producing the information. (See the next section.)

What factors are relevant to allocating costs?

In cases involving a large amount of ESI, or ESI that is not available from reasonably accessible sources, the costs to the producing party of locating the information, reviewing it for responsiveness and privilege, and otherwise preparing it for production may be very high.[15] At

15. Processing and reviewing ESI is thought to constitute about 94% of the total cost of its production. The cost range to review 100 gigabytes of information is estimated to be $7,000 to $284,375, a difference of $277,375, and the cost range to process 100 gigabytes of information, $75,000 to $180,000, a difference of $105,000. David Degnan, *Accounting for the Cost of Electronic Discovery,* 12 Minn. J. L. Sci. & Tech. 151 (2012). One hundred gigabytes of information is approximately equivalent to 100 small trucks, or a library floor, filled with books. Shira A. Scheindlin, Daniel J. Capra, & Kenneth J. Withers, Electronic Discovery and Digital Evidence 43 (West American Casebook Series 2008). Recently the Rand Corporation examined e-discovery costs in 35 cases and found dramatically higher review costs of $1,800 to

the same time, the cost of copying and transporting the information is greatly reduced, and the costs to the requesting party of searching or organizing the information may be reduced because it can be done electronically.

In such cases, it may be appropriate to shift at least some of the production costs from the producing party to the requesting party. Although Rule 26(b)(2)(B) does not contain explicit language authorizing cost shifting, the Advisory Committee note to the rule clearly anticipates the shifting of costs of producing information that is not reasonably accessible.[16] Two major cases—*Rowe Entertainment, Inc. v. William Morris Agency, Inc.*[17] and *Zubulake v. UBS Warburg LLC*[18]—introduced multifactor tests for determining when cost shifting is appropriate. Other courts have adopted or modified the *Rowe* and *Zubulake* formulations.

In *Rowe*, a racial discrimination case, the defendants objected to the production of e-mail information from backup media on the grounds that such discovery was unlikely to provide relevant informa-

---

$21,000 per gigabyte, with a median cost of $13,636 and a mean of $22,280. Nicholas M. Pace & Laura Zakaras, Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery (Rand Institute for Civil Justice, April 2012). Differences between the estimates in the two studies might be accounted for by the different data sources and study methods they used. The range of cost estimates within and between the two studies suggests the need for a comprehensive empirical examination of the cost of e-discovery.

16. Some courts have interpreted Rule 26(b)(2)(B) as requiring a showing of inaccessibility for cost shifting. *See, e.g.,* Peskoff v. Faber, 240 F.R.D. 26, 31 (D.D.C. 2007) ("*[A]ccessible* data must be produced at the cost of the producing party; cost-shifting does not even become a possibility unless there is first a showing of inaccessibility.") (emphasis in original); *accord* Pipefitters Local No. 636 Pension Fund v. Mercer Human Res. Consulting, Inc., 2007 WL 2080365, at *2 (E.D. Mich. July 19, 2007). Other courts have held, however, that Rule 26(c) provides judges with the authority to shift costs as part of enforcing proportionality limits. *See, e.g.,* Thompson v. U.S. Dep't of Housing and Urban Dev., 219 F.R.D. 93, 98 (D. Md. 2003) ("The options available are limited only by the court's own imagination and the quality and quantity of the factual information provided by the parties to be used by the court in evaluating the Rule 26(b)(2) factors. The court can, for example, shift the cost, in whole or part, of burdensome and expensive Rule 34 discovery to the requesting party . . . .").

17. 205 F.R.D. 421 (S.D.N.Y. 2002), *aff'd*, 53 Fed. R. Serv. 3d 296 (S.D.N.Y. 2002).

18. 217 F.R.D. 309 (S.D.N.Y. 2003).

tion and would invade the privacy of nonparties, and they requested that the plaintiffs bear the costs if production was nevertheless required. The court concluded that the e-mail information sought by the plaintiffs was relevant and that a blanket order precluding its discovery was unjustified. However, balancing eight factors derived from case law, the court required the plaintiffs to pay for the recovery and production of the e-mail backups, except for the cost of screening for relevance and privilege. The eight *Rowe* factors were as follows:

1. the specificity of the discovery requests;
2. the likelihood of discovering critical information;
3. the availability of such information from other sources;
4. the purposes for which the responding party maintains the requested data;
5. the relative benefit to the parties of obtaining the information;
6. the total cost associated with production;
7. the relative ability of each party to control costs and its incentive to do so; and
8. the resources available to each party.[19]

Zubulake, a sex discrimination case, also involved the production of e-mail messages that existed only on backup tapes and other archived media. After concluding that the plaintiff's request was relevant to her claims, the court held that the usual rules of discovery generally apply when the data are in accessible format, but that cost shifting could be considered when data were relatively inaccessible, such as on backup tapes. The court substituted seven different, though quite similar, factors for the *Rowe* factors:

(1) [t]he extent to which the request is specifically tailored to discover relevant information;

(2) [t]he availability of such information from other sources;

(3) [t]he total cost of production, compared to the amount in controversy;

(4) [t]he total cost of production, compared to the resources available to each party;

19. 205 F.R.D. at 428–29.

(5) [t]he relative ability of each party to control costs and its incentive to do so;

(6) [t]he importance of the issues at stake in the litigation; and

(7) [t]he relative benefits to the parties of obtaining the information.[20]

The court emphasized that the factors should not be applied mechanistically and should be weighted according to their importance.

Zubulake also set forth a sensible approach for assessing costs when a large amount of ESI that is not reasonably accessible is involved. *Zubulake* involved 77 backup tapes. Following the order in that case, the defendants restored and reviewed 5 of the tapes and found approximately 600 messages deemed to be responsive at a cost of about $19,000. Based on this work, the defendants were able to estimate the cost of restoring and reviewing the entire 77-tape collection. Considering the seven factors, the court determined that the balance tipped slightly against cost shifting, and it required the defendants to bear 75% of the restoration cost.[21]

How may Rule 26(g) sanctions be used to promote cooperation and proportionality in ESI discovery?

When signing discovery requests, responses, and objections under Rule 26(g), an attorney represents that they are "neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action."[22] A judge's close supervision of ESI discovery and the judge's availability to resolve disputes promptly are the most effective ways to keep the scope of discovery proportional to the case and to encourage cooperation among the parties. However, when necessary, sanctions for disproportionate or uncooperative discovery tactics can help curb abuses and encourage attorneys to be more thoughtful about the legitimacy of discovery requests, responses, and objections.

---

20. 217 F.R.D. at 322.

21. This case is commonly referred to as *Zubulake III*, 216 F.R.D. 280 (S.D.N.Y. 2003).

22. Fed. R. Civ. P. 26(g)(1)(B)(iii).

What principles apply to discovery from nonparties under Rule 45?

Discovery from nonparties is likely to be more frequent when the parties are seeking ESI than when they are seeking paper documents. Many businesses and individuals depend on telecommunications companies, Internet service providers, and computer network owners for computer services, and these non-parties may be the source for relevant and discoverable ESI, especially e-mail and text messages. There has been an explosion of online services, which may be rich repositories of discoverable ESI in a wide variety of cases. Social media, such as Facebook and LinkedIn, are possible sources of discovery in personal injury, employment discrimination, libel, and other types of cases. Organizations, both public and private, routinely outsource their computer-management and data-storage functions to "cloud computing" contractors and consultants, often without fully considering the consequences for records management and access.

Rule 45 of the Federal Rules of Civil Procedure conforms the rules on ESI discovery from third parties to those on ESI discovery from parties. Rule 45 introduces the concept of sources that are not reasonably accessible. It addresses the form or forms for the production of ESI, adds a post-production procedure for asserting claims of privilege or of protection as trial-preparation materials, and allows for the testing or sampling of ESI. Although Rule 45 has no equivalent to the Rule 26(f) conference process, parties seeking discovery from nonparties under Rule 45 should be encouraged to meet informally with nonparty respondents and to discuss the scope of the subpoena, the form in which ESI will be produced, protection against waiver for privileged and protected information, and the allocation of discovery costs.[23] Some courts have embodied such a requirement in guidelines, protocols, or local rules. For example, item 5 in the District of Kansas Guidelines for the Discovery of Electronically Stored Information, provides the following:

> Parties issuing requests for ESI from nonparties should attempt to informally meet and confer with the non-party (or counsel, if rep-

23. *See, e.g.,* Universal Delaware, Inc. v. Comdata Corp., No. 07-1078, 2010 WL 1381225 (E.D. Pa. Mar. 31, 2010) (addressing ESI in the subpoena context).

> resented). During this meeting, counsel should discuss the same issues with regard to requests for ESI that they would with opposing counsel as set forth in paragraph 4 above.[24]

Nonparty discovery—and, on occasion, discovery from parties—can be complicated by the Stored Communications Act (SCA).[25] Enacted in 1986 as part of the Electronic Communications Privacy Act,[26] and thus predating the pervasiveness of the Internet, the SCA establishes various definitions of providers of communications services and prohibits or limits disclosures of ESI. Attempts to enforce subpoenas on providers of services can be barred or limited by the SCA.[27]

A related issue, the discussion of which is beyond the scope of this guide, involves transnational discovery, that is, discovery sought from sources that are maintained in another country. Information in a foreign country may be subject to "blocking," data protection, or privacy statutes that prohibit the export or even simple collection of that information. In ruling on discovery requests or disputes, judges should be aware that under such statutes, penal sanctions may be levied against a producing party by the host country if these prohibitions are not obeyed.

In what form or forms should ESI be produced?

ESI can be produced in a variety of forms or formats, each with distinct advantages and disadvantages. The form of production may affect how easily, if at all, the receiving party can electronically search the information, whether relevant information is obscured or sensitive information is revealed, and how the information can be used in later stages of the litigation. For example, ESI can be produced as a TIFF or PDF file, which is essentially a photograph of an electronic document. Alternatively, ESI can be produced in "native format," that is, the form in which the information was created and is used in the normal course of the producing party's activities. Part 2 of *Effective*

24. District of Kansas Guidelines, *supra* note 8.

25. 18 U.S.C. §§ 2701–2712.

26. Pub. L. No. 99-508, 100 Stat. 1848 (1986).

27. For a decision interpreting the SCA and collecting authorities, see *Crispin v. Christian Audigier, Inc.,* 717 F. Supp. 2d 965 (C.D. Cal. 2010).

Use of Courtroom Technology[28] reviews in depth the various digital formats in which documents, photographs, videos, and other materials can be produced and the related issues of cost and usability.[29] Many decisions have now addressed form or forms of production.[30]

Rule 34 addresses the issue of the form of ESI and recognizes that different forms of production may be appropriate for different types of ESI and for different purposes for which the information is needed. It permits the requesting party to designate the form or forms in which it wants ESI produced, and it requires the responding party to identify the form in which it intends to produce the information if the requesting party does not specify a form or if the responding party objects to a form that the requesting party specifies. It also requires the parties to meet and confer if there is a dispute about form of production and provides that in the absence of a party agreement or court order, the responding party must produce ESI either in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable. The Advisory Committee note is clear that production of ESI in a form that removes or significantly degrades the recipient's ability to search the information electronically generally does not fulfill the "reasonably usable" requirement.

The judge should ensure that the parties discuss the form or forms of production at the Rule 26(f) conference and, if necessary, inform the court of any disputes at the Rule 16 conference. The parties should discuss the forms in which the ESI likely to be sought in discovery is available; which forms would meet the needs of the requesting party; and the associated costs, burdens, and problems of preserving and producing the ESI in a particular form. If the responding party believes it is necessary to translate requested information from the form in which it is ordinarily maintained into another reasonably usable form, the parties should discuss whether this form significantly reduces the requesting party's ability to search the information electronically and whether it makes it more difficult for the requesting

28. Effective Use of Courtroom Technology: A Judge's Guide to Pretrial and Trial (Federal Judicial Center 2001).

29. Also see the term *file format* in the Glossary to this guide.

30. *See, e.g.,* Aguilar v. Immigration & Customs Enforcement Div. of U.S. Dep't of Homeland Sec., 255 F.R.D. 350 (S.D.N.Y. 2008).

party to use the information efficiently in the litigation. The parties should also discuss any information, technical support, or other assistance the responding party may need to provide to the requesting party so that it can use the information.

In resolving disputes over the form or forms of production, the judge should consider the following:

1. What alternative forms are available? What are their benefits and drawbacks for the requesting and responding parties?
2. How difficult will it be for a responding party to preserve, collect, review, and produce ESI in the form requested?
3. If the responding party is not producing ESI in the form in which it is ordinarily maintained, is the party producing it in a form that is reasonably usable by the requesting party?
4. If the requesting party disputes that the proposed form of production is reasonably usable, what limits its use? Has the responding party stripped features, such as searchability, or metadata or embedded data that may be important? If so, what is the justification?

How should privilege and waiver issues be handled?

The volume of ESI that must be searched and produced in response to a discovery request can be enormous, and characteristics of certain types of ESI (e.g., embedded data, threads of e-mail communications, and e-mail attachments) also make it difficult to review for privilege and work-product protection. Thus, the risk of inadvertent disclosure of privileged or protected material during production persists even if great care is taken to identify and segregate it.

What are "clawback" and "quick peek" agreements?

To facilitate discovery, parties sometimes enter into agreements that help minimize the risk of waiver by inadvertent disclosure. Under what is commonly called a "clawback" agreement, the responding party typically reviews the material for privilege or protection before it is produced, but the parties also agree to a procedure for the return of privileged or protected information that is inadvertently produced. Alternatively, under "quick peek" agreements, which have been

used less frequently, the responding party provides requested material without a thorough review for privilege or protection, but with the explicit understanding that making it available to the requesting party does not waive any privilege or protection that may apply. The requesting party must sort through the material and designate under Rule 34 the specific documents it would like formally produced. The responding party then has the opportunity to review the documents that have been specifically requested and withhold those that are asserted to be privileged or protected.

How can a court shield parties from waiving a privilege through inadvertent disclosure?

Given the increased likelihood of inadvertent production of privileged or protected ESI and the increased cost and delay required for effective preproduction review, the judge should encourage parties to discuss whether they can agree to "clawback," "quick peek" or similar arrangements. If the parties are able to agree, the court should include their agreement in the case-management order or in a separate order. Once the court has incorporated the parties' agreement in an order, the litigants are protected against assertions by third parties in parallel or subsequent cases that privilege or work-product protection has been waived through inadvertent disclosure in this litigation.[31] See the discussion of Federal Rule of Evidence 502(d) *infra* pages 26–27.

How should a court test assertions of privilege?

Any assertion of privilege raises the question of how that assertion is to be tested. The accepted practice is, of course, in camera inspection of the material by the judge. In cases involving ESI, however, the judge may have to decide whether the sheer volume of information requires new methods of review, such as sampling or, in the rare case, the use of a special master.[32]

---

31. In the absence of an agreement between the parties or a court order, Federal Rule of Civil Procedure 26(b)(5)(B) establishes a default procedure for asserting privilege after production.

32. Federal Rule of Civil Procedure 26(b)(5)(A), generally speaking, requires the production of a privilege log. Such logs can be problematic at best when large quantities of ESI need to be listed, in particular, e-mail threads. Innovative approaches to

How is Federal Rule of Evidence 502 used to reduce cost and delay?

Because of ESI's volume and mutability, its review for privilege can be time-consuming and costly. Federal Rule of Evidence 502 should help to reduce these burdens, and courts should encourage its use.

Rule 502, adopted in 2008, limits the waiver of attorney–client privilege or work-product protection by inadvertent disclosures. Most important for ESI discovery management, Rule 502(d) allows a court to order that production in the case will not waive privilege or work-product protection.

Under Rule 502(a), an inadvertent disclosure of privileged ESI during a federal proceeding can never result in *subject matter waiver* at either the federal or state level. This alleviates the concern of producing parties that the innocent or minimal disclosures that are common in ESI discovery operate as a waiver of privilege not only as to what was produced but as to the entire subject matter.

Under Rule 502(b), inadvertent disclosure in a federal proceeding does not operate as a waiver in a federal or state proceeding if the holder of the privilege took reasonable steps to prevent the disclosure and promptly took reasonable steps to rectify the error, including following the procedures set forth in Federal Rule of Civil Procedure 26(b)(5)(B). Rule 502(b) sought to establish a uniform standard across the United States courts for determining whether inadvertent production results in privilege waiver.[33]

Subsection (d) is in many ways the heart of Rule 502. It allows the court, on a party's motion or sua sponte, to enter an order providing

---

logging ESI alleged to be privileged can be found in John M. Facciola & Jonathan M. Redgrave, *Asserting and Challenging Privilege Claims in Modern Litigation: The Facciola-Redgrave Framework*, 4 Fed. Ct. L. Rev. 19 (2009), and J. A. Thomas et al., *Reducing the Costs of Privilege Reviews and Logs*, Nat'l L.J., March 23, 2009, at S1.

33. Federal Rule of Evidence 502(b) provides an objective way to determine if remedial measures are reasonable by referencing Federal Rule of Civil Procedure 26(b)(5)(B), but leaves defining the standard for determining the "reasonableness" of preventive measures completely to the courts. For decisions addressing the "reasonableness" of such steps, see, for example, *Amobi v. District of Columbia Department of Corrections,* 262 F.R.D. 45 (D.D.C. 2009); *Relion, Inc. v. Hydra Fuel Cell Corp.,* No. CV06-607, 2008 WL 5122828 (D. Or. Dec. 4, 2008); and *Rhoads Industries, Inc. v. Building Materials Corp. of America,* 254 F.R.D. 216 (E.D. Pa. 2008).

that production of materials in connection with a federal proceeding will not waive privilege or work-product protection. The order is enforceable not only between the parties in that case but also as to third parties and in other state or federal proceedings. Rule 502(e) underscores the importance of incorporating party agreements on the effect of disclosure into a court order so that the waiver protection will extend to third parties and other cases. Party agreements not incorporated in a court order are binding *only* as between the parties.

The protection available under Rule 502 applies even in state courts. The provisions in Rule 502(b) regarding inadvertent disclosures in federal proceedings and Rule 502(d) nonwaiver orders in federal proceedings are binding in related state proceedings. Rule 502(c) speaks to the effect of disclosures in a state proceeding on privilege assertion in federal courts.

With these provisions, parties should be more willing to enter into "quick peek" agreements, which reduce review costs even more than the more commonly used "clawback" agreements. Rule 502 obviates the need for exhaustive preproduction review to the extent it is motivated by a party's fear of waiving privilege or protection. Judges should encourage parties to consider all reasonable approaches for reducing the burdens of privilege review at their Rule 26(f) conference. For example, an order might allow search-and-retrieval experts on both sides to meet, confer, and compare results of test searches without fear of forfeiting privilege. If parties fail to reach an agreement about production and waiver, the court may enter the Rule 502(d) order on its own to remove the risk of waiver through inadvertent production.[34]

Litigation holds: How can the court promote the parties' reasonable efforts to preserve ESI?

Because of ESI's dynamic, mutable nature, it is extremely important for parties to discuss its preservation early in the case, and the judge should raise the issue if the parties do not do so in a timely manner. In many cases, preservation obligations arose even before the complaint

34. *See* Rajala v. McGuire Woods, LLP, No. 08-2638-CM-DJW, 2010 WL 2949582 (D. Kan. July 22, 2010) (the court, over the objections of the plaintiff, entered an order with a "clawback" provision, as requested by the defendant).

was filed. The parties and the court should balance the need to preserve relevant information with the need to continue computer operations critical to a party's routine activities. The preservation steps required should be reasonable and proportional to the particular case.

The judge may help ensure that parties avoid later allegations of spoliation by requiring them to discuss, and reviewing with them, steps for establishing and implementing an effective preservation plan. Such steps can be incorporated into case-management orders or discovery protocols and may include

1. having a knowledgeable person describe the party's information systems, storage, and retention policies and practices to the opposing party and the court;
2. interviewing key employees to determine sources of information;
3. affirmatively and repeatedly communicating litigation holds to all affected employees and other persons and monitoring compliance on an ongoing basis;
4. integrating discovery responsibilities with routine data retention policies and practices;
5. actively managing and monitoring document collections; and
6. documenting the steps taken to design, implement, and audit the litigation hold.[35]

Some of the existing ESI discovery protocols go into great detail about the scope, duration, and implementation of litigation holds. See, for example, the District of Maryland Protocol (paragraph 7) and the District of Delaware Default Standard (paragraph 1), discussed *infra* note 44 and accompanying text.

Early in the case, particularly where there is an identified risk that potentially relevant ESI will be lost, the judge should urge the parties to discuss and reach agreement on preservation. An agreement on what categories or sources of ESI will be preserved minimizes the risk that relevant evidence will be deliberately or inadvertently destroyed,

35. This list is based on the discussion in *Zubulake V*, 229 F.R.D. 422 (S.D.N.Y. 2004), and is illustrated in detail in *Pension Committee of University of Montreal Pension Plan v. Banc of America Securities, LLC,* 685 F. Supp. 2d 456 (S.D.N.Y. 2010).

helps ensure that information is retrieved when it is most accessible (i.e., before it has been deleted or removed from active online data), and helps protect the producing party from later spoliation allegations. The agreement may be incorporated into a court order if the parties feel that would be helpful or necessary to ensure enforcement.

Any such order must be both clear and narrowly drawn, however. The order should clearly define the preservation obligations and should be narrowly drawn to avoid imposing burdens that may unduly interfere with a party's day-to-day operations or creating "gotcha" situations by requiring preservation steps that are unrealistic or difficult to follow.[36] In crafting the order, the judge needs to learn from the responding party what data-management systems are routinely used, the volume of data affected, and the costs and technical feasibility of implementing the order. Such orders should ordinarily include provisions that permit the destruction of information under specified circumstances. An order may, for example, exclude from preservation requirements specified categories of documents or data whose costs of preservation substantially outweigh their relevance to the litigation, particularly if the information can be obtained from other sources. Moreover, as issues in the case are narrowed, the judge may ask the parties if the preservation order should be revisited and reduced in scope.

Two other considerations may be helpful to judges in dealing with preservation issues. First, actors other than the parties may become important. These actors may be the custodians of ESI relevant to a proceeding and may be bound by contractual relationships with parties to create and/or maintain the ESI. The duty to preserve ESI may well extend to such nonparty actors.[37] Second, as technology advances and automated litigation-related tools become more widely available and more reliable and cost-effective to use, courts may hold parties

36. The *Manual for Complex Litigation, Fourth* provides guidance about what type of preservation order is most useful and under what circumstances an order should be entered. *See* MCL 4th, *supra* note 2, § 11.442.

37. For decisions addressing preservation obligations that may be imposed on nonparty consultants, see, for example, *Cedar Petrochemicals, Inc. v. Dongbu Hannong Chemical Co.,* 769 F. Supp. 2d 269 (S.D.N.Y. 2011); *Goodman v. Praxair Services, Inc.,* 632 F. Supp. 2d 494 (D. Md. 2009); and *Innis Arden Golf Club v. Pitney Bowes, Inc.,* 257 F.R.D. 334 (D. Conn. 2009).

to standards of preservation (and production) that reflect those advances and tools.

What are the standards for finding spoliation and the criteria for imposing sanctions?

The flip side of data preservation is, of course, spoliation. Spoliation is the destruction or material alteration of evidence or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation. The authority to impose sanctions for spoliation arises under the Federal Rules of Civil Procedure and, if the rules do not apply, the court's inherent powers. Determining whether sanctions are warranted for spoliation of ESI often presents a challenge to a court, given the ease with which ESI can be either intentionally or inadvertently deleted or modified.

The case law on sanctions for spoliation of ESI is growing and beyond the scope of this introductory guide. In determining what sanctions to impose, a judge should look to the controlling circuit law and the facts of the case. How relevant was the evidence lost, and to what extent did its destruction prejudice the opposing party? Was the destruction of evidence the result of negligence or gross negligence, or was it intentional and in bad faith? Was the information destroyed for the purpose of preventing its use in the litigation, or unintentionally as a result of the good-faith operation of the computer system? Depending on the importance of the lost or modified information to the claims or defenses, on the party's level of culpability, and on the controlling circuit law,[38] a variety of sanctions may be imposed. These

38. See the appendix to *Victor Stanley, Inc. v. Creative Pipe, Inc.,* 269 F.R.D. 497 (D. Md. 2010), which is a chart that describes positions on spoliation and sanctions taken by each court of appeals and includes related citations. Two decisions are illustrative of the differing approaches courts of appeals have taken. In *Pension Committee of University of Montreal Pension Plan v. Banc of America Securities, LLC,* 685 F. Supp. 2d 456 (S.D.N.Y. 2010), styled "*Zubulake* Revisited: Six Years Later," the court considered the imposition of spoliation sanctions under Second Circuit law and determined that monetary sanctions were appropriate for negligence, but an adverse instruction, in addition to monetary sanctions, was appropriate for gross negligence. In comparison, the court in *Rimkus Consulting Group v. Cammarata,* 688 F. Supp. 2d 598 (S.D. Tex. 2010), held that under Fifth Circuit law, severe sanctions, such as adverse inferences, may not be imposed unless evidence of bad faith exists.

range in severity from monetary sanctions to preclusion of evidence or adverse inferences and to dismissal of the complaint or entry of default. A common theme in the case law is that the least severe sanction responsive to the spoliation should be imposed. Even if a sanction is not appropriate, courts may order additional discovery to redress the unavailability of information that was not preserved.

Considerations regarding spoliation of ESI and sanctions

Relevance of evidence lost and extent of prejudice

Degree of culpability

Relationship to records-management policy and Rule 37(e)

One common feature of computer systems is the deletion of outdated or ephemeral information on an ongoing, prescheduled basis to prevent overloading the system (e.g., overwriting deleted digital information, recycling backup tapes, and purging e-mail messages after a certain period). Rule 37(e) acknowledges such record-management policies, stating that "*absent exceptional circumstances*, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, *good-faith* operation of an electronic information system" (emphasis added). The issue of "good faith" may be complicated. Good faith may require, among other things, a party to modify or suspend certain features of the electronic information system to prevent the loss of information subject to a preservation order, and it may preclude a party from exploiting the routine operation of the system to avoid the party's discovery obligations. The phrase "absent exceptional circumstances" provides the court with flexibility to respond to the facts of each case.

Where can a judge find additional information and guidance?

Many resources on ESI exist—there are resources for a judge who is managing a case involving significant amounts of ESI for the first time, for a judge who is confronted with a complex ESI issue, and for a court that wants to develop a uniform ESI policy through local rules, guidelines, or protocols. The Federal Judicial Center maintains materials on electronic discovery on its intranet and Internet sites.[39]

39. http://cwn.fjc.dcn/fjconline/home.nsf/pages/196 and http://www.fjc.gov/public/home.nsf/pages/196.

The 2006 amendments to the Federal Rules of Civil Procedure that specifically address the discovery of ESI and the associated Advisory Committee notes offer considerable guidance in managing the discovery of ESI, as does Federal Rule of Evidence 502, which was adopted in 2008. The growing body of case law concerning ESI-related discovery is also useful; a quarterly summary prepared by The Sedona Conference is available on the Center's resource page. In addition, the *Manual for Complex Litigation, Fourth* provides assistance on some matters, such as preservation orders.

Some professional associations have devoted considerable attention to ESI discovery issues and offer a wealth of information for judges. See, for example, *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production* (The Sedona Conference Working Group Series June 2007);[40] *The Sedona Conference Cooperation Proclamation: Resources for the Judiciary* (August 2011);[41] and *Managing E-Discovery and ESI: From Pre-Litigation Through Trial,* published in 2011 by the American Bar Association.[42]

Courts, too, have been proactive in developing guidance on ESI discovery. The Seventh Circuit Electronic Discovery Pilot Program was initiated in May 2009 as a multiyear, multiphase process to develop, implement, evaluate, and improve pretrial litigation procedures that provide fairness and justice to all parties while reducing the cost and burden of electronic discovery, consistent with Rule 1 of the Federal Rules of Civil Procedure. The program's Phase 1 Report sets forth eleven principles relating to the discovery of ESI. From October 2009 through March 2010, these principles were tested in practice; thirteen judges of the U.S. District Court for the Northern District of Illinois (five district judges and eight magistrate judges) implemented them in 93 civil cases. An interim report on Phase 2 of the program presents slightly revised principles, reflecting the experience of these judges, as well as results from surveys of both judges and attorneys. The re-

40. The Sedona Principles, *supra* note 2.

41. http://www.thesedonaconference.org/dltForm?did=Judicial_Resources.pdf.

42. Michael D. Berman, Courtney Ingraffia Barton & Paul W. Grimm, Managing E-Discovery and ESI: From Pre-Litigation Through Trial (American Bar Association 2011).

ports; a model standing order embodying the principles; a list of the district, magistrate, and bankruptcy judges participating in Phase 2 of the program; and other material on the program's website offer much insight.[43]

In addition, some courts, such as the U.S. District Courts for the District of Delaware, District of Kansas, and District of Maryland, have adopted guidelines or protocols for dealing with ESI discovery issues.[44] These protocols provide a useful starting place for developing district-wide guidelines or for developing case-management orders in individual cases. For example, the stated purpose of the Maryland Protocol is to provide parties with a comprehensive, yet flexible, framework for facilitating the just, speedy, and inexpensive conduct of discovery involving ESI in civil cases, and to promote, whenever possible, the resolution of disputes regarding the discovery of ESI without the court's intervention. It is detailed enough for the most complex case, yet adaptable for cases that may involve small stakes and comparatively small amounts of ESI. The court encourages attorneys to follow the protocol, as is appropriate to their cases, and indicates that it might consider compliance with the protocol in resolving discovery disputes and imposing sanctions. The protocol encourages parties to hold a meaningful Rule 26(f) conference (or conferences) to discuss issues relating to the disclosure and discovery of ESI, and to submit a report to the court embodying their agreements and disagreements and proposed treatment of ESI that is subject to attorney–client privilege and work-product protection. The protocol also provides detailed guidance to parties in preparing for the conference.

Other courts have adopted local rules to address an assortment of ESI-related issues. For example, Local Rule 26.1 for the Middle District of Pennsylvania describes the preparation expected of attorneys before the Rule 26(f) meeting of counsel, the issues related to ESI that

43. Seventh Circuit Electronic Discovery Pilot Program, http://www.discoverypilot.com.

44. District of Delaware Default Standard, *supra* note 5; District of Kansas Guidelines, *supra* note 8; District of Maryland Protocol, *supra* note 4. *See also* Federal Circuit Advisory Council Model Order, *supra* note 9. A collection of guidelines, protocols, and local rules can be found on the Federal Judicial Center's Materials on Electronic Discovery page at http://cwn.fjc.dcn/fjconline/home.nsf/pages/196 and http://www.fjc.gov/public/home.nsf/pages/196.

should be discussed at the meeting, and how points of disagreement should be presented to the court. It also generally describes the disclosures of ESI that are expected under Rule 26(a)(1.)

Conclusion

Discovery of ESI presents new and unique challenges to litigants, lawyers, and judges. The challenges include scope, allocation of costs, form or forms of production, waiver of privilege and work-product protection, and preservation and spoliation. To effectively manage these issues, judges must understand the relevant technology at a level that allows effective communication with attorneys, parties, and experts. The information in this guide is an introduction to the issues, and additional resources can be found on the Center's intranet and Internet sites.

To facilitate efficient and cost-effective discovery, judges must require attorneys to take seriously their obligation to meet and confer under Rule 26(f) and to submit a meaningful discovery plan that addresses ESI issues likely to arise in the case. Judges must also encourage parties to narrowly target requests for ESI. Judges must evaluate whether the costs of complying with the requests are proportional to the benefit of complying. To this end, judges may need to impose limits on discovery; encourage or order tiered or stayed discovery; order sampling to determine the relevance, need, and cost of more expansive discovery; or shift costs from the producing party to the requesting party, particularly when information that is not reasonably accessible must be produced. Judges need to help ensure that ESI is produced in a usable form, and they may need to clarify the procedures to be followed if privileged or protected information is inadvertently disclosed. They should help parties balance the need to preserve relevant evidence with the need to continue routine computer operations critical to a party's activities, and enter preservation orders as appropriate.

In the end, judges must actively manage electronic discovery, raising points for consideration by parties rather than waiting for parties to present disputes that can delay a case, add to its costs, and distract from its merits. Such active management can help ensure the expeditious and fair conduct of discovery involving ESI.

Glossary

Most entries in this glossary were derived, with permission, from *The Sedona Conference Glossary: E-Discovery & Digital Information Management* (3d ed. 2010), *available at* https://thesedonaconference.org/download-pub/471.

active data (active records): Information located in a computer system's memory or in storage media attached to the system (e.g., disk drives) that is readily available to the user, to the operating system, and to application software. (See *storage medium*.)

application: One or more related software programs that enable a user to enter, store, view, modify, or extract information from files or databases. The term is commonly used in place of *program* or *software*. Applications may include word processors, Internet browsing tools, spreadsheets, e-mail clients, personal information managers (contact information and calendars), and other databases.

archival data: Information that is maintained in long-term storage for business, legal, regulatory, or similar purposes, but not immediately accessible to a computer system's user. The data may be stored on removable media, such as CDs, tapes, or removable disk drives, or may be maintained on system disk drives. The data are typically stored in an organized way to help identify, access, or retrieve individual records or files.

attachment: A record or file associated with another record for the purpose of retention, transfer, processing, review, production, or routine records management. There may be multiple attachments associated with a single "parent" or "master" record. In many records and information management programs, or in a litigation context, the attachments and associated records may be managed and processed as a single unit. In common use, this term often refers to a file (or files) associated with an e-mail message for retention and storage as a single message unit.

backup data (disaster recovery data): An exact copy of data that serves as a source for recovery in the event of a system problem or disaster. The data are generally stored separately from active data on tapes or removable disk drives, and often without indexes or other information. As a result, the data are in a form that makes it difficult to identify, access, or retrieve individual records or files.

backup tape recycling: A process in which backup data tapes are overwritten with new backup data, usually according to a fixed schedule determined jointly by records-management, legal, and information technology (IT) personnel.

cloud computing: "[A] model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." http://csrc.nist.gov/groups/SNS/cloud-computing/ (last visited June 22, 2010). For further explanation, see the NIST website cited.

computer forensics: The scientific examination and analysis of computerized data primarily for use as evidence. Computer forensics may include the secure collection of computer data; the examination of suspect data to determine details, such as origin and content; and the presentation of computer-based information to courts. It may involve re-creating deleted, damaged, or missing files from disk drives; validating dates and authors or editors of documents; and certifying key elements of electronically stored information.

data (electronic): Information stored on a computer, including numbers, text, and images. Computer programs (e.g., word processing software, spreadsheet software, presentation software) are used to process, edit, or present data.

data mining: Generally refers to knowledge discovery in databases (structured data). It relies on automatic and semiautomatic techniques to extract previously unknown interesting patterns from large quantities of data, which can then be subjected to further inspection and analysis. In the context of electronic discovery, this term often refers to the processes used to sort through a collection of electronically stored information to extract evidence for production or presentation in an investigation or in litigation.

de-duplication: A process that searches for and deletes duplicate information. (See the glossary maintained by The Sedona Conference for a description of different types of de-duplication.)

deleted data: Data that once existed on a computer as active data, but have been marked as deleted by computer programs or user activity. Deleted data may remain on the storage media in whole or in part until they are overwritten or "wiped." Even after the data have been wiped, directory entries, pointers, or other information relating to the deleted data may remain on the computer.

deletion: A process in which data are marked as deleted by computer programs or user activity and made inaccessible except through the use of special data-recovery tools. Deletion makes data inaccessible with normal application programs, but commonly leaves the data on the storage medium. There are different degrees of deletion. "Soft-deleted data" are data marked as deleted in the computer operating system (and not generally available to the user after such marking), but not yet physically removed from or overwritten on the storage medium. Soft-deleted data can often be restored in their entirety. In contrast, "wiping" is a process that overwrites the deleted data with random digital characters, rendering the data extremely difficult to recover, and "degaussing" is a process that rearranges the magnetic patterns on the medium, rendering the data impossible to recover with all but the most sophisticated computer forensics tools.

disk mirroring: The ongoing process of making an exact copy of information from one location to another in real time. It is often used to protect data from a catastrophic hard disk failure or for long-term data storage. (See *replication*.)

electronic discovery: The process of collecting, preparing, reviewing, and producing electronic documents in a variety of criminal and civil actions and proceedings.

embedded data: Data that include commands that control or manipulate data, such as computational formulas in spreadsheets or formatting commands in a word processing document. Embedded data are not visible when a document is printed or saved as an image format. (See *metadata*.)

ESI: Electronically stored information.

file format: The internal organization, characteristics, and structure of a file that determine the software programs with which it can optimally be used, viewed, or manipulated. The simplest file format is ASCII (American Standard Code for Information Interchange; pronounced "ASK-ee"), a nonproprietary text format. Documents in ASCII consist of only text with no formatting or graphics and can be read by most computer systems using nonproprietary applications. Specific applications may define unique (and proprietary) formats for their data (e.g., WordPerfect document file format). These formats are also called the "native" format. Files with unique formats may only be viewed or printed with their originating application or an application designed to work with compatible formats. Computer systems commonly identify files by a naming convention that denotes the native format

(and therefore the probable originating application) as an extension of the file's name. For example, a WordPerfect document could be named document.wpd, where ".wpd" denotes a WordPerfect file format. Other common formats are .docx for Microsoft Word files, .xls for Microsoft Excel spreadsheet files, .txt for ASCII text files, .ppt for Microsoft PowerPoint files, .jpg for photographs or other images, and .pdf for Adobe Acrobat documents.

forensic copy: An exact copy of an entire physical storage medium (e.g., hard drive, CD, DVD, tape), including all active and residual data and unallocated, or slack, space on the medium. Forensic copies are often called "images" or "imaged copies."

form of production: The manner in which requested documents are produced. The term is used to refer to both the file format and the media on which the documents are produced (paper versus electronic).

hash value: A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical identifiers so distinctive that the chance that any two data sets will have the same one, no matter how similar they appear, is less than one in one billion. "Hashing" is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production.

image (verb): To image a hard drive is to make an identical copy of the hard drive at the lowest level of data storage. The image will include deleted data, residual data, and data found in hidden portions of the hard drive. Imaging is also known as creating a "bit stream image" or "mirror image," or "mirroring" the drive. It is different from the process of making a "logical copy" of or "ghosting" a hard drive, which normally copies only the active data on the hard drive, and not the deleted data, residual data, and data in hidden portions of the hard drive.

legacy data: Electronically stored information in which an organization may have invested significant resources and which retains importance, but which was created and is stored through the use of software and/or hardware that has become obsolete or replaced ("legacy systems"). Legacy data may be costly to restore or reconstruct.

metadata: Information about a particular data set or document which describes how, when, and by whom the data set or document was collected, created, accessed, or modified; its size; and how it is formatted. Some meta-

data, such as file dates and sizes, can easily be seen by users; other metadata can be hidden from users but are still available to the operating system or the program used to process the data set or document. (See *embedded data* and *systems data*.)

near-line data storage: Storage in a system that is not physically part of the computer system or local network in daily use, but can be accessed through the network. Near-line data may be stored in a library of CDs, which can be automatically located and loaded for reading, or stored at a remote location accessible through an Internet connection. There is usually a small time lag between the request for data stored in near-line media and the data's availability to an application or user. Making near-line data available is an automated process (in contrast, making "offline" data available generally can be done only by a person physically retrieving the data).

offline data storage: The storage of electronic records, often for long-term archival purposes, on removable media (e.g., CDs, removable disk drives) or magnetic tape that is not connected to a computer or network. Accessing offline media usually requires manual intervention and is much slower than accessing online or near-line media.

PDF (portable document format): A file format developed by Adobe Systems Incorporated. Once converted to this format, documents are readable outside of the application that created them. A PDF file captures document formatting information (e.g., margins, spacing, fonts) from the original application (e.g., WordPerfect) in such a way that the document can be viewed and printed as intended in the original application by the Adobe Reader program, which is available for most computer operating systems. Other programs (most notably Adobe Acrobat) are required to edit or otherwise manipulate a PDF file.

records management: The activities involved in handling information, generally for organizations that are large data producers. Records management includes maintaining, organizing, preserving, and destroying information, regardless of its form or the medium on which it is stored.

replication: The ongoing process of making an exact copy of information from one location to another in real time. It is often used to protect data from a catastrophic failure or for long-term data storage. (See *disk mirroring*.)

residual data (ambient data): Data that are not active on a computer system and that are not visible without the use of "undelete" or other special

data-recovery techniques. Residual data may contain copies of deleted files, Internet files, and file fragments.

restore: To transfer data from a backup or archival storage system (e.g., tapes) to an online system. Restoring archival data may require replication of the original hardware and software operating environment.

sampling: The process of selecting a small part of a larger data source and searching it to test for the existence, or frequency, of relevant information, to assess whether the source contains privileged or protected information, and to assess the costs and burdens of identifying and producing requested information.

search engine: A program that enables a search for key words or phrases, such as on web pages throughout the World Wide Web. (See the glossary maintained by The Sedona Conference for a description of different types of searches.)

storage medium: The physical device containing electronically stored information, including computer memory, disk drives (including removable disk drives), magneto-optical media, CDs, DVDs, memory sticks, and tapes.

systems data: Information about a computer system that includes when people logged on and off a computer or network, the applications and passwords they used, and what websites they visited.

This page is left blank intentionally to facilitate printing of this document double-sided.

The Federal Judicial Center

About the Federal Judicial Center

The Federal Judicial Center is the research and education agency of the federal judicial system. It was established by Congress in 1967 (28 U.S.C. §§ 620–629), on the recommendation of the Judicial Conference of the United States.

By statute, the Chief Justice of the United States chairs the Center's Board, which also includes the director of the Administrative Office of the U.S. Courts and seven judges elected by the Judicial Conference.

The organization of the Center reflects its primary statutory mandates. The Education Division plans and produces education and training programs for judges and court staff, including video programs, publications, curriculum packages for in-court training, and Web-based programs and resources. The Research Division examines and evaluates current and alternative federal court practices and policies. This research assists Judicial Conference committees, who request most Center research, in developing policy recommendations. The Center's research also contributes substantially to its educational programs. The two divisions work closely with two units of the Director's Office—the Information Technology Office and the Communications Policy & Design Office—in using print, broadcast, and online media to deliver education and training and to disseminate the results of Center research. The Federal Judicial History Office helps courts and others study and preserve federal judicial history. The International Judicial Relations Office provides information to judicial and legal officials from foreign countries and assesses how to inform federal judicial personnel of developments in international law and other court systems that may affect their work.