FEDERAL JUDICIAL CENTER
POCKET GUIDE SERIES

Managing Discovery of Electronic Information

Third Edition

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

Federal Judicial Center
2017

FIRST PRINTING

Contents

Preface

This third edition of the pocket guide on managing the discovery of electronically stored information (ESI) reflects the December 1, 2015, amendments to the Federal Rules of Civil Procedure and the reasons for the amendments described by Chief Justice Roberts in the *2015 Year-End Report on the Federal Judiciary*:

> (1) encourage greater cooperation among counsel; (2) focus discovery—the process of obtaining information within the control of the opposing party—on what is truly necessary to resolve the case; (3) engage judges in early and active case management; and (4) address serious new problems associated with vast amounts of electronically stored information.[1]

The prevalence of ESI led to the December 1, 2006, amendments to the Federal Rules of Civil Procedure. Those amendments have been the bedrock for countless decisions in the U.S. courts. In 2008, Federal Rule of Evidence 502 was adopted to, among other things, address the consequences of inadvertent disclosure of ESI on claims of attorney–client privilege and work-product protection.

The third edition also reflects the rise of new devices on which ESI is created and stored, such as smartphones, and new sources of ESI, such as social media. It updates judges on how ESI may be searched. It also suggests case-management techniques that judges might use in smaller civil actions in which the costs of ESI discovery could hamper resolution on the merits.

This pocket guide is organized into a question-and-answer format, which we hope judges will find useful in meeting the challenges presented by the discovery of ESI as it becomes a routine feature in litigation. The guide's fundamental message

1. Chief Justice John G. Roberts, Jr., 2015 Year-End Report on the Federal Judiciary 5 (2015).

remains unchanged from the first edition: 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.

The insightful comments of Judge Cheryl A. Eifert (S.D. W. Va.), Judge Xavier Rodriguez (W.D. Tex.), Judge Craig B. Shaffer (D. Colo.), and Kenneth J. Withers (The Sedona Conference) were invaluable in producing this edition, as was the research assistance and editorial assistance of Jessica Snowden, Geoffrey Erwin, and Alexander Cranford. Many others commented on both the first and second editions of the pocket guide, and we gratefully acknowledge their enduring influence on this edition.

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

ESI currently includes email messages, word-processing files, webpages, and databases that are 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). Increasingly, ESI is stored on cloud-based servers (hosted by third parties) that are accessed through Internet connections. Technology changes rapidly, making a complete list impossible. Federal Rules of Civil Procedure 26 and 34, effective as of December 1, 2006, use the broad term "electronically stored information" to identify a distinct category of information that, along with "documents" and "tangible things," is subject to discovery rights and obligations.

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 of production
- Dependence on the system that created it
- Deleting doesn't necessarily delete it

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 flash drives; 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 nearly 2.5 million 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 email 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.[2] 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 email, the history of its transmission. Metadata are created for some 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.

Unlike paper documents, ESI can be produced in different forms, such as PDF (portable document format) and TIFF (tagged image file format). Some forms may not be compati-

2. Definitions for technical terms such as metadata, embedded data, and systems data are in the glossary to this guide. Most entries in this glossary were derived, with permission, from *The Sedona Conference Glossary: E-Discovery & Digital Information Management (Fourth Edition*), 15 Sedona Conf. J. 305 (2014), *available at* https://thesedonaconference.org/download-pub/3757 (last visited May 3, 2017).

ble 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 available, either because it is obsolete or 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. Retrieving and restoring such information, however, can be expensive and can require extensive effort.

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?

Discovery involving word-processing documents, spreadsheets, email, and other ESI is commonplace. Once seen primarily in large actions involving sophisticated entities, it is now routine in civil actions and is increasingly seen in criminal actions.[3] In many cases, ESI does not raise any issue. In some cases, ESI is converted 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.

Issues to anticipate, manage, and resolve

- Scope and proportionality
- Form of production
- Attorney–client privilege and work-product protection
- Preservation and spoliation
- Cost shifting
- Admissibility

Through early and sustained case management, judges can help ensure attorneys and parties cooperate and work together, and with the court, in controlling the expense and time demands of discovery—an obligation given effect in the 2015 amendments.[4] Such cooperation also will help minimize

3. For information about ESI in criminal cases, see Sean Broderick, Donna Lee Elm, Andrew Goldsmith, John Haried & Kiran Raj, *Criminal e-Discovery: A Pocket Guide for Judges* (Federal Judicial Center 2015). Also, a collection of state and federal cases and related materials is maintained on the website for the Attorney General of Massachusetts, http://www.mass.gov/ago/bureaus/criminal/emcc/the-cyber-crime-division/electronic-information.html (last visited May 3, 2017).

4. "Cooperation" is not new to the Federal Rules of Civil Procedure. Parties and their attorneys have long been required to cooperate in the preparation of the Rule 26(f) discovery plan and to confer in good faith to avoid the need to bring motions for protective orders under Rule 26(c)(1) and to compel disclosures or discovery under Rule 37(a)(1). Amended Rule 1 heightens the obligation of attorneys and parties to cooperate through-

disputes by encouraging lawyers and parties to identify and resolve, 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 the disputes quickly and that the judge resolves the disputes 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 cases that are complex or contentious, or in which the volume of ESI subject to discovery is large, these responsibilities are not easy undertakings. Disputes that are difficult, time-consuming, and costly to resolve may arise as to the scope of discovery of ESI; 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; and whether inadvertent production of ESI waives 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 should raise such issues for the parties to consider rather than wait for the issues to be presented as full-blown disputes.

Another issue that might arise is the admissibility of ESI produced in discovery or derived from discovery materials, a full discussion of which is outside the scope of this guide. In

---

out all phases of litigation, and, as Chief Justice Roberts observed, "work cooperatively in controlling the expense and time demands of litigation—an obligation given effect in the amendments that follow. The new passage highlights the point that lawyers—though representing adverse parties—have an affirmative duty to work together, and with the court, to achieve prompt and efficient resolutions of disputes." Roberts, *supra* note 1, at 6.

brief, judges should encourage the parties to cooperate during discovery and at the pretrial stage to address admissibility issues and eliminate or minimize the need for motion practice in advance of trial or in limine. Judges are "gatekeepers" of admissibility under Federal Rule of Evidence 104(a). They may be presented with disputes about the admissibility of ESI per se as well as the admissibility of ESI-derived testimony. Disputes may include, among other things, whether ESI-related testimony should be characterized as opinion testimony under Evidence Rule 701 or expert testimony under Evidence Rule 702, whether ESI can be authenticated under Evidence Rules 901 or 902, or whether ESI is hearsay under Evidence Rules 801–807. Moreover, disputes may be centered on new or novel sources of ESI, such as content on social media (United States v. Browne, 834 F.3d 403 (3d Cir. 2016)) or satellite images and digital "tacks" labeled with GPS coordinates (United States v. Lizarraga-Tirado, 789 F.3d 1107 (9th Cir. 2015)).

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 issues, judges have found it appropriate to seek the assistance of a special master or neutral expert.[5]

---

5. 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 (2004) [hereinafter MCL 4th] *and* The Sedona Principles (Second Edition): Best Practices Recommendations & Principles for Addressing Electronic Document Production, at Comment 10.c (The Sedona Conference Working Group Series, June 2007), *available at* https://thesedonaconference.org/download-pub/81 (last visited May 3, 2017) [hereinafter The Sedona Principles]. The draft of a third

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 Federal Rule of Civil Procedure 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 also can indicate to parties how to bring disputes before the court for efficient and prompt resolution. Rule 16(b)(3)(B)(v), effective in 2015,

Tools to promote early consideration of ESI

- Informed, meaningful, and ongoing Rule 26(f) conferences
- Informal resolution of matters via Rule 16(b)(3)(B)(v)
- Early Rule 34 requests via Rule 26(d)(2)
- Rule 16 conference and initial scheduling order

edition of the Principles was published for public comment in March 2017, https://thesedonaconference.org/download-pub/5120 (last visited May 3, 2017).

provides one means for more informal resolution of such matters: in the initial scheduling order, include a provision that prior to filing a discovery-related motion a party "must request a conference with the court." Some judges who hold such conferences find them an efficient way to resolve discovery disputes without the process of a formal motion.

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 36–40). 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 intranet site (http://fjc.dcn) and its Internet site (http://fjc.gov).

The December 1, 2015, amendments offer another avenue for active case management at the earlier stage of civil litigation. Rule 26(d)(2) now provides:

> (A) *Time to Deliver*. More than 21 days after the summons and complaint are served on a party, a request under Rule 34 may be delivered:
>
> (i) to that party by any other party, and
>
> (ii) by that party to any plaintiff or to any other party that has been served.
>
> (B) *When Considered Served.* The request is considered as to have been served at the first Rule 26(f) conference.

A judge might encourage this practice in select civil actions, perhaps complex ones, as a way to focus the parties on proportional written discovery. Should the parties not reach agreement as to scope at the Rule 26(f) meet-and-confer, the

judge will then have an opportunity to provide guidance and, if necessary, make rulings on scope via the initial Rule 16 conference and scheduling order. Whether this practice is productive depends on whether it is reasonable to expect the parties to be prepared to serve focused discovery requests at an early stage in the litigation. In any event, judges should recognize that any guidance or rulings might be provisional.

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

Federal Rule of Civil Procedure 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;
- whether proposed discovery will be proportional to the needs of the case;
- 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;
- what the scope of preservation should be in terms of temporal duration, source, and form or forms;
- the steps each party will take to preserve different types or categories of ESI;[6]

6. Specific discussion topics related to the preservation of information are listed in the *MCL 4th*, *supra* note 5, § 40.25(2).

- 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;
- 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 email 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.[7]

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

7. Judges might also direct the attention of attorneys to Ariana J. Tadler, Kevin S. Brady & Karin Scholz Jenson, *The Sedona Conference "Jumpstart Out-*

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 36–40).

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 15–17). 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 usually 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 the information. 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 *Principles for the Discovery of Electronically Stored Information in Civil Cases*

---

line": Questions to Ask Your Client & Your Adversary to Prepare for Preservation, Rule 26 Obligations, Court Conferences & Requests for Production (Mar. 2016), *available at* https://thesedonaconference.org/download-pub/4683 (last visited May 3, 2017).

provides detailed guidance to parties in preparing for the Rule 26(f) conference. Among other things, the principles suggest that parties engage in cooperative exchanges about ESI at the earliest stages of litigation and that counsel discuss who will participate with their clients and each other to ensure the participation of one or more persons for each party who are well-informed concerning the potentially relevant systems and data.[8]

The District of Maryland Principles also enumerate the type of information parties consider exchanging to inform conferences and agreements between the parties. These include

- a data map (either in list form or visual) and information about the following types of technologies, systems, tools, or protocols as used by the parties: software applications or platforms, including databases; document management, mail, and messaging systems;
- types of computing devices (including portable computing and storage devices);
- use of home computers or personally-owned devices;
- the identity and rights of individuals to access the systems and specific files, services, and applications;
- network and database design and structure;
- use of cloud, off-site, or other third-party services, including social media and personal email; and
- backup and recovery routines, including backup media rotation practices.[9]

Another useful exchange might be organizational charts for key custodians of ESI and relevant policies, including those relating to computer usage, document management, ESI, or document retention or destruction. There are two kinds of

8. U.S. District Court for the District of Maryland, Principles for Discovery of Electronically Stored Information in Civil Cases, Principles 1.02 and 2.02, *available at* http://www.mdd.uscourts.gov/sites/mdd/files/ESI-Principles.pdf (last visited May 3, 2017) [hereinafter District of Maryland Principles].

9. *Id.*, Principle 1.02.

custodians: those with substantive knowledge of content and those with knowledge about systems.

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.

What matters should be covered during the Rule 16 conference and included in the initial scheduling order?

The Rule 16 conference 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 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 the attorneys 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 of trial-preparation material after production. Of course, the order will also include other key provisions, including 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 if they have 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.[10]

How should a judge manage ESI in a small case?

Cooperation and proportionality are central to the successful management of small civil actions in which the cost of e-discovery might exceed the value of the litigation. In a smaller case, a judge's pretrial interaction with attorneys may occur only at the Rule 16 conference or when a discovery dispute arises. Useful management techniques, in addition to those described above, might include

- engaging the parties at the Rule 16 conference about the value of the action and what ESI might be sought and at what expense;
- setting a short discovery period and an early trial date to focus the parties on what is really needed from each other to prepare for trial;
- allowing any discovery disputes to be presented in an informal manner pursuant to Rule 16(b)(3)(B)(v) (as amended December 2015); and
- encouraging the parties to enter into stipulations pursuant to Rule 29(b) in lieu of discovery and into nonwaiver agreements embodied in orders under Federal Rule of Evidence 502.[11]

10. *See, e.g.*, *id.*, Principle 2.02.

11. For additional guidance for small cases, see Gill S. Freeman, Paul S. Grewal, Ronald J. Hedges & Craig B. Shaffer, *Active Management of ESI in "Small" Civil Actions,* FMJA Bulletin (Jan. 2014), *available at* http://www.fedbar.org/Image-Library/Chapters/Hawaii-Chapter/ACTIVE-MANAGEMENT-OF-ESI-IN-SMALL-CIVIL-ACTIONS.aspx?FT=.pdf (last visited May 3, 2017).

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

Federal Rule of Civil Procedure 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) does not 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."[12] While not required by the letter of the rule, a party's initial disclosure should identify the nature of its computer systems, including its backup system, network system, and email system and the software applications used by them.[13]

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, allowing parties to forgo Rule 26(a)(1) disclosures can be problematic. If the parties want to forgo Rule 26(a)(1) disclosures, they should present the court with a realistic alternative procedure for exchanging baseline information about the relevant

12. Fed. R. Civ. P. 26 advisory committee's note to 1993 amendment.

13. *Compare* J. M. Moore, Moore's Federal Practice § 37A.20[2] (3d ed. 2010) (stating an exhaustive search of inaccessible sources is not required as part of the initial disclosure obligation) *with* U.S. District Court for the District of Kansas, Guidelines for Cases Involving Electronically Stored Information [ESI], http://www.ksd.uscourts.gov/guidelines-for-esi/ (last visited May 3, 2017) [hereinafter District of Kansas Guidelines] (suggesting the search include "current, back-up, archival, and legacy computer files").

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, administered, and employed by the court and the parties 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.

The addition of the phrase "and employed by the court and the parties" in 2015 further emphasizes, as described in the Advisory Committee note, "that just as the court should construe and administer these rules to secure the just, speedy, and inexpensive determination of every action, so the parties share the responsibility to employ the rules in the same way." 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)(1), as amended in 2015, sets out the proportionality factors in defining the scope of discovery, thus reinforcing the obligation of parties to consider these factors in making discovery requests, responses, or objections. They include

- "importance of the issues at stake";
- "amount in controversy";

- "relative access to relevant information";
- "the parties' resources";
- "importance of the discovery"; and
- "burden or expense . . . outweighs its likely benefit."

Rules 26(f) and 16(b) explicitly reference preservation as a subject to be considered by parties *and* judges at the earliest stage of litigation. This early consideration is essential when dealing with ESI, given its potential volume, variety, and location, and the effect that preservation might have on a party's daily operations. Assuming no dispute exists about the date on which the duty to preserve was triggered, the judge should engage the parties about what is being preserved and whether the parties can agree on the proper scope of preservation. In this regard, it should be noted that *scope* has two aspects, one "temporal" and the other, for lack of a better term, "spatial."

Temporal is relatively straightforward: To what time period does a duty to preserve extend in terms of the claims and defenses of a particular civil action? For example, a letter threatening litigation was found sufficient to trigger a duty to preserve in *Matthew Enterprise, Inc. v. Chrysler Group LLC,* No. 13-cv-04236, 206 WL 2957133 (N.D. Cal. May 23, 2016).

The spatial scope of preservation is amorphous. As described below, there are certain types of ESI that might be of marginal relevance, at best. These types might include ESI that is "dynamic" in nature, such as an interactive website, the content of which is not ordinarily retained, or ESI that is in the possession of a third party (e.g., a social media provider). The parties should be encouraged to discuss at the Rule 26(f) conference whether *everything* needs to be preserved or whether a more limited scope of preservation would be consistent with the goals of amended Rule 1 and the needs of the case.[14]

14. Case law on preservation in the context of proportionality is sparse. There are a few decisions in which judges have ordered that costs be shared. One decision approved the disposal of computers as an exer-

Whether the proportionality requirement of Rule 26(b)(1) 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. 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 those 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 email searches is often tangential to the central issues in patent litigation.[15]

Systems data, which include such information as the time users logged on and off a computer or network, the applications and passwords they used, and what websites they visited, may be more remote and costlier to produce. Other types

---

cise of proportionality. Lord Abbett Mun. Income Fund, Inc. v. Asami, 2014 WL 5477639, at *3 (N.D. Cal. Oct. 29, 2014). After the entry of final judgment and while an appeal was pending, a party sought to dispose of computers. *Id.* at *1. The court found that the parties opposing disposal declined the opportunity to inspect the computers or share in storage costs and that the computers did not contain relevant ESI. *Id.* at *2–3.

15. *See* The Advisory Council for the United States Court of Appeals for the Federal Circuit, An E-Discovery Model Order, http://www.cafc.uscourts.gov/sites/default/files/announcements/Ediscovery_Model_Order.pdf (last visited May 3, 2017) [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), https://www.fjc.gov/sites/default/files/materials/2017/CostCiv1.pdf (last visited May 3, 2017). The order promotes the exchange of core documentation concerning the patent, the accused product, the prior act, and the finances before email production requests are made. It requires email production requests to be focused on a specific issue, and presumptively limits the number of custodians and search terms for such requests.

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 created on now-obsolete computer systems.[16]

To ensure that the proportionality requirement is met, 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.

Staged discovery

Initial search focused on key players and events, expanded as necessary based on results

Easily accessible sources first, expanded as necessary, then less-accessible sources

Sampling of less-accessible sources to evaluate benefits

When hard-to-access information is of potential interest, the judge should encourage or require the 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 the parties to sample ESI that is not reasonably accessible to better evaluate whether the benefits of a full search and of retrieving and restoring the ESI will justify the associated costs and burdens.

The judge also may be called upon to require or allow a mirror image of ESI. If so, the judge may need to consider

16. *See, e.g.*, Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 318–20 (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).

matters of relevance, proportionality, privacy, and confidentiality, particularly where the holder of the ESI is a third party.[17]

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 these actions 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."[18] 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.

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.[19] A judge might require, among other things, an affidavit from a person with

17. For an explanation of mirroring, see the term *image* in the glossary, *infra*.

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

19. 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*, 14 Sedona Conf. J. 155 (2013), *available at* https://thesedonaconference.org/download-pub/1778 (last visited May 3, 2017).

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 accessible. The Seventh Circuit Pilot Project Proposed 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.[20]

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 knowl-

20. Seventh Circuit Electronic Discovery Committee, [Proposed] Standing Order Relating to the Discovery of Electronic Evidence, at 5 (Principle 2.04(d)), http://www.discoverypilot.com/sites/default/files/StandingOrde8_10.pdf (last visited May 3, 2017).

edgeable about the responding party's information systems;[21] 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.[22]

The Advisory Committee note on the amendment 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

(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 email communications rele-

21. *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).

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

vant to a disputed contract may have all occurred several years ago and are 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 following 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.[23] At 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.

---

23. 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 (2011). 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 45 (West American Casebook Series 2012). The Rand Corporation examined e-discovery costs in 36 cases and found higher review costs of $1,766 to $209,899 per gigabyte, with a median cost of $13,636 and a mean of $22,480. Nicholas M. Pace & Laura Zakaras, Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery (Rand Institute for Civil Justice, Apr. 2012), *available at* http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1208.pdf (last visited May 3, 2017). 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.

In such cases, it may be appropriate to shift at least some of the production costs from the producing party to the requesting party. Judges have inherent power to order that costs be shifted or shared.[24] As described below, some uncertainty arose as to the scope of that power after the December 1, 2006, amendments. This led to the December 1, 2015, amendment of Rule 26(c)(1)(B) that, for good cause, a judge could allocate "expenses." Before the 2015 amendments, some courts interpreted Rule 26(b)(2)(B) as requiring a showing of inaccessibility for cost shifting.[25]

Two major cases—*Rowe Entertainment, Inc. v. William Morris Agency, Inc.*[26] and *Zubulake v. UBS Warburg LLC*[27]—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 email information from backup media on the grounds that such discovery was unlikely to provide relevant information and would invade the privacy of

---

24. *See Civil Rules Advisory Committee Note to Proposed Amendment to Rule 34(b),* 181 F.R.D. 18, 89–91 (1998); 8 Fed. Prac. & Proc. Civ. § 2008.1 (2016).

25. *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 Hous. & 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 . . . .").

26. 205 F.R.D. 421 (S.D.N.Y. 2002), *aff'd*, 53 Fed. R. Serv. 3d 296 (S.D.N.Y. 2002).

27. 217 F.R.D. 309 (S.D.N.Y. 2003).

nonparties, and they requested that the plaintiffs bear the costs if production was nevertheless required. The court concluded that the email 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 email 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.[28]

Zubulake, a gender discrimination case, also involved the production of email 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 an accessible format, but that cost shifting could be considered when data are 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;

28. *Rowe*, 205 F.R.D. at 428–29.

> 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;
>
> 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.[29]

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 five 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.[30]

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. For computer services, many businesses and individuals depend on telecommunications companies, Internet service providers, and computer network owners, and these

29. *Zubulake*, 217 F.R.D. at 322.

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

nonparties may be the source for relevant and discoverable ESI, especially email 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, Twitter, 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.

Federal Rule of Civil Procedure 45 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.[31] Some courts have embodied such a requirement in guidelines, protocols, or local rules. For example, paragraph 26 in the District of Kansas Guidelines for the Discovery of Electronically Stored Information provides the following:

> Counsel issuing requests for ESI from non-parties should attempt to informally meet and confer with the non-party (or counsel, if represented). During this meeting, counsel should discuss the same issues regarding ESI requests that

31. *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).

> they would with opposing counsel as set forth in Paragraph 11 above [regarding Rule 26(f) conference obligations generally].[32]

Nonparty discovery—and, on occasion, discovery from parties—can be complicated by the Stored Communications Act (SCA).[33] Enacted in 1986 as part of the Electronic Communications Privacy Act,[34] 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.[35]

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 preservation and 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.[36]

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

---

32. District of Kansas Guidelines, *supra* note 13.

33. 18 U.S.C. §§ 2701–2712.

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

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

36. Timothy P. Harkness, Rahim Moloo, Patrick Oh & Charline Yim, Discovery in International Civil Litigation: A Guide for Judges (Federal Judicial Center 2015); The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery and Data Protection*, 17 Sedona Conf. J. 397 (2016), *available at* https://thesedonaconference.org/download-pub/4789 (last visited May 3, 2017).

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 II of *Effective Use of Courtroom Technology*[37] 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.[38] Many decisions have addressed form or forms of production.[39]

Is information in . . .
The form specified by the requesting party?
Ordinarily maintained form?
Reasonably useful form?
Searchable form?
Form that retains relevant information, including metadata or embedded data?
Form that masks, as appropriate, sensitive information?
Efficient form for later litigation stages?

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. Rule 34 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 provides that in the absence of a party agreement or court order, the re-

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

38. Also see the term *file format* in the glossary, *infra*.

39. *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).

sponding 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 to the 2006 amendment 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, that the parties 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 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. Rule 26(c) and Rule 37(a) regarding motions for protective orders and motions to compel, respectively, both require parties to certify that they have conferred or attempted to confer in good faith in an effort to resolve the dispute without court action.

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, metadata, or embedded data, that may be important? If so, what is the justification?

How might data be searched to respond to discovery requests or subpoenas?

At least in theory, a court need not know how a party conducts a search for data in response to a request made under Federal Rule of Civil Procedure 34(b). However, parties must confer and report on disclosure and discovery of information pursuant to Rule 26(f)(3)(C) and other orders issued pursuant to Rule 26(f)(3)(F), and the court may be required to address related disputes at the initial Rule 16 conference. Moreover, search may become an issue when a party challenges the adequacy and completeness of an adversary's production.[40] Parties may dispute how a search *should* be conducted and, after the fact, how a search *should have been* conducted.[41] Absent compromise by the parties, the court

40. Similar disputes may arise when a subpoena is served on a nonparty for the production of data pursuant to Rule 45(a)(1)(C).

41. When confronted with disputes about the search for ESI in the possession, custody, or control of a party or subpoenaed nonparty, judges might benefit from reading *The Sedona Conference Commentary on Defense of Process: Principles and Guidelines for Developing and Implementing a Sound E-Discovery Process* (Public Comment Version Sept. 2016), *available at* https://thesedonaconference.org/download-pub/4815 (last visited May 3, 2017). This commentary "addresses the tension between the principle of

may be asked to order the use of a particular search tool or methodology.

Anyone who has conducted an Internet search probably has a basic understanding of how parties conduct electronic searches of data to respond to discovery requests. Data can be searched manually, of course, either by review of printed pages (in which instance metadata will be unsearchable) or of data on a screen. Given that data may be voluminous and only a small portion of that data may include responsive material, however, parties may use a variety of tools to conduct electronic searches. These can include techniques known as keyword search, concept search, discussion threading, clustering, find similar, and near-duplicate identification.

Currently, the most sophisticated search tool is technology-assisted review (TAR), also known as computer-assisted review and predictive coding. TAR is defined as a process for prioritizing or coding a collection of electronically stored information using a computerized system that harnesses human judgments of subject-matter experts on a smaller set of documents and then extrapolates those judgments to the remaining documents in the collection.[42] A broad discussion of TAR is beyond the scope of this guide.[43] The limited case law on TAR has either (a) approved the use of a TAR tool agreed-on by parties[44] or (b) addressed one party's attempt to use

---

party-controlled discovery, and the need for accountability in the discovery process" and suggests means to address this tension. *Id.* at iii.

42. Maura R. Grossman & Gordon V. Cormack, *The Grossman-Cormack Glossary of Technology-Assisted Review*, 7 Fed. Cts. L. Rev. 1 (2013).

43. For more information about TAR, see Timothy Lau & Emery G. Lee III, Technology-Assisted Review for Discovery Requests: A Pocket Guide for Judges (Federal Judicial Center 2017) and *The Sedona Conference TAR Case Law Primer*, 18 Sedona Conf. J. ___ (forthcoming), *available at* https://thesedonaconference.org/download-pub/5023 (last visited May 3, 2017).

44. *See* Da Silva Moore v. Publicis Groupe & MSL Grp., 287 F.R.D. 182 (S.D.N.Y. 2012); Rio Tinto PLC v. Vale S.A., 306 F.R.D. 125 (S.D.N.Y. 2015).

TAR over an adversary's objection.[45] Courts should be aware that a contested hearing on the use of a TAR tool or the "outcome" of TAR in a civil action may require expert testimony under Federal Rule of Evidence 702.

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 email communications, and email 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 the material.

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.

45. *See* Bridgestone Americas, Inc. v. IBM, No. 3:13-1196, 2014 WL 4923014 (M.D. Tenn. July 22, 2014).

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. Only once the court has incorporated the parties' agreement in an order are the litigants 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.[46] See the discussion of Federal Rule of Evidence 502(d), *infra* pages 38–40.

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.[47]

---

46. 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.

47. 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. Innovative approaches to 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 (2010), and J. A. Thomas et al., *Reducing the Costs of Privilege Reviews and Logs*, Nat'l L.J., Mar. 23, 2009, at S1.

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), disclosure of privileged ESI during a federal proceeding will not result in *subject-matter waiver* at either the federal or state level, unless the party intentionally put protected information into the litigation in a selective, misleading, and unfair manner. 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 or work-product waiver.[48]

48. 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. D.C. 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.

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 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. A 502(d) order might read:

> 1. The production of privileged or work-product protected documents, electronically stored information ('ESI') or information, whether inadvertent or otherwise, is not a waiver of the privilege or protection from discovery in this case or in any other federal or state proceeding. This Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d).
> 2. Nothing contained herein is intended to or shall serve to limit a party's right to conduct a review of documents, ESI or information (including metadata) for relevance, responsiveness and/or segregation of privileged and/or protected information before production.[49]

Rule 502(e) underscores the importance of incorporating into a court order party agreements on the effect of disclosure 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 state proceedings. Rule 502(c) speaks to the effect of disclosures in a state proceeding on privilege assertion in federal courts.

Dec. 4, 2008); and *Rhoads Industries, Inc. v. Building Materials Corp. of America*, 254 F.R.D. 216 (E.D. Pa. 2008).

49. U.S. District Court for the Southern District of New York, Rule 502(d) Order, http://www.nysd.uscourts.gov/cases/show.php?db=judge_info&id=928 (last visited May 3, 2017).

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 may obviate 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.[50]

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 ESI 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 arise even before the complaint is 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 by reviewing with them, steps for establishing and implementing an effective preservation plan. Such steps can be incorpo-

50. *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).

rated into case-management orders[51] 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.[52]

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 Principles, the District of Kansas Guidelines, and the District of Delaware Default Standard for Discovery.[53]

---

51. The 2015 amendments to Rule 16(b)(3)(B) added three items to the permitted contents of scheduling orders, including (1) the preservation of electronically stored information, a topic also added to the provisions of a discovery plan under Rule 26(f)(3)(C), and (2) agreements incorporated in a court order under Rule 502 controlling the effects of disclosure of information covered by attorney–client privilege or work-product protection, a topic also added to the provisions of a discovery plan under Rule 26(f)(3)(D). The order may also direct that before filing a discovery-related motion, the movant request a conference with the judge.

52. This list is based on the discussion in *Zubulake v. UBS Warburg LLC* (*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).

53. District of Maryland Principles, *supra* note 8, Principle 2.01; District of Kansas Guidelines, *supra* note 13, Paragraph 8; U.S. District Court for the

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, 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.[54] 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

---

District of Delaware, Default Standard for Discovery, Including Discovery of Electronically Stored Information ("ESI"], Paragraph 1(c) and Schedule A [hereinafter District of Delaware Default Standard], *available at* http://www.ded.uscourts.gov/sites/default/files/Chambers/SLR/Misc/EDiscov.pdf (last visited May 3, 2017).

54. 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 5, § 11.442.

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.[55] 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 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, the loss of data that might give rise to spoliation. Spoliation is the destruction or material alteration of evidence or the failure to preserve physical objects (including paper)[56] once a duty to preserve attaches. The authority to impose sanctions for spoliation of data comes from Federal Rule of Civil Procedure 37(e), which was substantially amended effective December 1, 2015. Sanction authority may also derive from other sections of Rule 37 and, assuming that a rule does not apply, from the

55. 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).

56. Amended Rule 37(e) applies *only* to the loss of data. Accordingly, case law before December 1, 2015, applies to the loss of physical objects such as paper, and that case law reflects a split among the circuits on, among other things, the level of scienter required for the imposition of spoliation sanctions and the availability of adverse inferences. See the 2012 edition of this guide at 30 & n.38.

inherent power of a court.[57] Determining whether sanctions, known as "remedial measures" under amended Rule 37(e), should be awarded and, if so, what sanctions should be imposed, is a challenge for a court and requires a case-by-case analysis of the alleged spoliator's state of mind, relevance of the lost data, prejudice to the opposing party, and the appropriate sanction. However, the analysis must begin with a determination of whether the alleged spoliator took "reasonable steps" to avoid the loss of the data in issue. If the court finds such steps were taken, the court should proceed no further under Rule 37(e).

The case law under amended Rule 37(e) is growing, and an analysis of it is premature and beyond the scope of this pocket guide. Basically, however, a step-by-step analysis under Rule 37(e) involves the following:

- Was there a duty to preserve the data in issue? If not, the analysis ends.
- Were reasonable steps taken to avoid the loss of the data? If so, the analysis ends.

---

57. The Advisory Committee Note to amended Rule 37(e) states that the rule preempts resort to inherent power. However, at least one court has noted in dicta that inherent power remains available. Cat3, LLC v. Black Lineage, Inc., 164 F. Supp. 3d 488, 497–98 (S.D.N.Y. 2016). Another court, however, followed the Advisory Committee Note. Living Color Enters., Inc. v. New Era Aquaculture, Ltd., No. 14-cv-62216, 2016 WL 1105297, at *4 & n.2 (S.D. Fla. Mar. 22, 2016). *Dietz v. Bouldin*, 579 U.S. ___ (2016), provides a helpful discussion of the inherent authority of federal judges to "manage their own affairs so as to achieve the orderly and expeditious disposition of [civil] cases." Two principles control: any exercise of such authority must be "a reasonable response to the problems and needs confronting the court's fair administration of justice," and the exercise must not be "contrary to any express grant of, or limitation on" a federal court's power "contained in a rule or statute." *Id.* Also, in *Goodyear Tire & Rubber Co. v. Haeger*, 581 U.S. ___ (2017), the Supreme Court considered a federal court's inherent authority to sanction a litigant for bad-faith conduct by ordering it to pay the other side's legal fees, holding that a causal link between the litigant's misbehavior and legal fees paid by the opposing party must be established.

- Can the lost data be "restored or replaced through additional discovery"? If so, the analysis ends.
- Was the other party prejudiced by the loss of the data? If not, the analysis ends.
- If there was prejudice, the court can impose "measures no greater than necessary to cure the prejudice." These measures can include, when warranted, allowing the injured party to comment on or introduce evidence about the lost data at trial.

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)

If data were lost "with the intent to deprive another party" of the use of the lost data, prejudice is assumed and the court can allow a permissive or mandatory adverse inference or impose a case-terminating sanction.[58]

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. As a starting point, the Federal Judicial Center maintains materials on electronic discovery, including many of those cited in this pocket guide and on its intranet (http://fjc.dcn) and Internet sites (http://fjc.gov).

58. There is an open issue as to whether the imposition of Rule 37(e)(2) sanctions requires proof by preponderance of the evidence or by clear and convincing evidence. *Compare* Cat3, LLC v. Black Lineage, Inc., 164 F. Supp. 3d 488 (S.D.N.Y. 2016) (clear and convincing), *with* Ramirez v. T&H Lemont, Inc., 845 F.3d 772 (7th Cir. 2016) (preponderance of the evidence).

The 2006 and 2015 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. 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);[59] *The Sedona Conference Cooperation Proclamation: Resources for the Judiciary* (December 2014);[60] and *Managing E-Discovery and ESI: From Pre-Litigation Through Trial,* published in 2011 by the American Bar Association.[61]

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 improve pretrial litigation procedures while reducing the cost and burden of electronic discovery, consistent with Rule 1 of the Federal Rules of Civil Procedure. The program's Phase One 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 the principles in 93 civil cases. The Phase Two

59. The Sedona Principles, *supra* note 5.

60. https://thesedonaconference.org/download-pub/3968 (last visited May 3, 2017).

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

report 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 reports are available on the program's website, along with a model standing order embodying the principles; a model discovery plan; a model case-management order; an interim report on Phase Three of the program; and other materials.[62]

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 principles for dealing with ESI discovery issues.[63] These documents provide a useful starting point for developing district-wide guidelines or for developing case-management orders in individual cases. For example, the stated purpose of the Kansas Guidelines 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. Emphasizing both proportionality and cooperation, the guidelines are detailed enough for the most complex case, yet adaptable for cases that may involve small stakes and comparatively small amounts of ESI.

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 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).

---

62. Seventh Circuit Electronic Discovery Pilot Program, http://www.discoverypilot.com/ (last visited May 3, 2017).

63. District of Delaware Default Standard, *supra* note 53; District of Kansas Guidelines, *supra* note 13; District of Maryland Principles, *supra* note 8. *See also* Federal Circuit Advisory Council Model Order, *supra* note 15.

Conclusion

Discovery of ESI can present unique challenges to litigants, lawyers, and judges, including those related to 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; 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. Judges 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 should enter preservation orders as appropriate.

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* (Fourth Edition), *available at* https://thesedonaconference.org/download-pub/3757 (last visited May 3, 2017).

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, email 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 email 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 May 3, 2017). 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 recreating 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 Microsoft Word document could be named document.docx, where ".docx" denotes a Microsoft Word file format. Other common formats are .pdf for Adobe Acrobat documents,.xls for Microsoft Excel spreadsheet files, .txt for ASCII text files, .ppt for Microsoft PowerPoint files, and .jpg for photographs or other images, and.

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 metadata, 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., Microsoft Word) 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 webpages 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.

The Federal Judicial Center

Board

The Chief Justice of the United States, *Chair*
Magistrate Judge Tim A. Baker, U.S. District Court for the Southern District of Indiana
Judge Curtis L. Collier, U.S. District Court for the Eastern District of Tennessee
Chief Judge Barbara J. Houser, U.S. Bankruptcy Court for the Northern District of Texas
Judge Kent A. Jordan, U.S. Court of Appeals for the Third Circuit
Judge Kimberly J. Mueller, U.S. District Court for the Eastern District of California
Judge George Z. Singal, U.S. District Court for the District of Maine
Judge David S. Tatel, U.S. Court of Appeals for the District of Columbia Circuit
James C. Duff, Director of the Administrative Office of the U.S. Courts

Director

Judge Jeremy D. Fogel

Deputy Director

John S. Cooke

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 for judges and court staff, including in-person programs, video programs, publications, curriculum packages for in-district 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 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 informs federal judicial personnel of developments in international law and other court systems that may affect their work. Two units of the Director's Office—the Information Technology Office and the Editorial & Information Services Office—support Center missions through technology, editorial and design assistance, and organization and dissemination of Center resources.