

How To Manage And Prepare For Electronic Discovery In Litigation

A. Electronic Discovery Rules.

The Federal Rules of Civil Procedure have long recognized technology's impact on discovery, and amendments to the Rules promulgated in 2015 updated how parties propound and respond to e-discovery requests. Further, ethical canons established in response to advances in technology and the prevalence of e-discovery in 21st Century litigation require lawyers to be fully familiar with a client's computer and data systems and social media. This section will cover the amended Federal Rules and rules of professional conduct that pertain to the discovery of electronically-stored information ("ESI").

[Rule 26](#) outlines federal litigation discovery:

(3) Discovery Plan. A discovery plan must state the parties' views and proposals on:

...

(C) any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced;

...

(E) what changes should be made in the limitations on discovery imposed under these rules or by local rule, and what other limitations should be imposed[.]

[FED. R. CIV. PROC. 26.](#)

[Federal Rule 34](#) long ago embraced the impact of changing technology on discovery. See Committee Note on Rule—1970 Amendment. In 2006, the Rule again recognized technology's influence on litigation:

Electronically stored information may exist in dynamic databases and other forms far different from fixed expression on paper. Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents.... The wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of electronically stored information. Rule 34(a)(1) is expansive and includes any type of information that is stored electronically. A common

[Read more on page 17](#)



Eric L. Probst, Esq.

Porzio Bromberg & Newman PC



How to Manage... continued from page 7

example often sought in discovery is electronic communications, such as e-mail. The rule covers—either as documents or as electronically stored information—information “stored in any medium,” to encompass future developments in computer technology.”

See Committee Note on Rule—2006 Amendment.

The 2015 amendments have again changed the Rule to address technology’s effect on discovery. [Federal Rule of Civil Procedure 34](#) now reads:

(a) In General. A party may serve on any other party a request within the scope of [Rule 26\(b\)](#):

(1) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party’s possession, custody, or control:

(A) any designated documents or *electronically stored information*—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form[.]

[FED. R. CIV. PROC. 34\(a\)\(1\)\(A\)](#). Counsel propounding e-discovery requests “must describe with reasonable particularity each item or category of items to be inspected,” and “may specify the form or forms in which electronically stored information is to be produced.” [Id. at 34\(b\)\(1\)\(A\)\(C\)](#). The producing party should object to any e-discovery requests that fail to satisfy the “reasonable particularity standard” of paragraph (A). See [id. at 34\(b\)\(2\)\(C\)](#). The producing party can also object to the form in which ESI will be produced. [Id. at 34\(b\)\(2\)\(D\)](#). The Rule also addresses how ESI will be produced:

(E) Producing the Documents or Electronically Stored Information. Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:

(i) A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request;

(ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in



which it is ordinarily maintained or in a reasonably usable form or forms; and

(iii) A party need not produce the same electronically stored information in more than one form.

Id. at 34(b)(2)(E).

The 2015 amendments attempt to remove discovery roadblocks objections to be stated with “specificity,” [FED. R. CIV. PROC. 34\(b\)\(2\)\(B\)](#), and to specify whether documents are being withheld based on the objection, [FED. R. CIV. PROC. 34\(b\)\(2\)\(C\)](#). The amendments also advise counsel to identify the category of documents being withheld from production based on an objection that the request is overbroad, and compels them to produce documents in response to the part of the individual document request that is not overbroad. See Committee Notes on Rule—2015 Amendment.

With the requirement that e-discovery requests be specifically tailored to the case, [Rule 26\(b\)\(1\)](#) imposes a proportionality requirement. [FED. R. CIV. PROC. 26\(B\)\(1\)](#).

(1) Scope in General. Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any non-privileged matter that is relevant to any party’s claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties’ relative access to relevant information, the parties’ resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

Proportionality levels the playing field in many cases and in others places the cost of e-discovery more fairly on the party requesting the production of wide-ranging categories of ESI.

The most significant amendment is 37(e)—Sanctions. The 2015 amendment replaced section 37(e) in its entirety and applies exclusively to ESI. The 2006 version of section 37(e) contained a “safe harbor” provision that protected a company from sanctions if electronically-stored material was lost through “the routine, good-faith operation of an electronic information system.” [FED. R. CIV. PROC. 37\(e\) \(2006\)](#). [37\(e\)](#) now reads:



(e) Failure to Preserve Electronically Stored Information. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:

(A) presume that the lost information was unfavorable to the party;

(B) instruct the jury that it may or must presume the information was unfavorable to the party; or

(C) dismiss the action or enter a default judgment.

[FED. R. CIV. PROC. 37\(e\) \(2016\)](#).

Lawyers' e-discovery obligations go beyond familiarity with the federal and local rules of civil procedure.. The 2012 Amendments to the ABA Model Rules of Professional Conduct reflect a lawyer's duty to embrace and understand evolving technology. [Rule 1.1](#), Competence, provides that, "[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." [ABA Model Rules of Professional Conduct, 1.1](#). Comment 8 to the 2012 Amendments—Maintaining Competence—highlights a lawyer's duty to understand technology: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject." *Id.* at comment 8 (emphasis supplied).

The impact of technology has reached the state level as state ethical guidelines impose similar obligations. See *New York State Bar Association 2015 Guidelines* ("A lawyer cannot be competent absent a working knowledge of the benefits and risks associated with the use of social media."). Further, New York requires lawyers to "keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information."



Comment [8] to [New York Rule of Professional Conduct 1.1](#). New York has also written into the Rules these definitions:

“Computer-accessed communication” means any communication made by or on behalf of a lawyer or law firm that is disseminated through the use of a computer or related electronic device, including, but not limited to, web sites, weblogs, search engines, electronic mail, banner advertisements, pop-up and pop-under advertisements, chat rooms, list servers, instant messaging, or other internet presences, and any attachments or links related thereto.

[New York Rules of Professional Conduct, Rule 1.0\(c\)](#). 23 states have adopted ABA Comment 8 to [Rule 1.1](#).¹

Ethical obligations have increased with the prevalence of data privacy issues. [Rule 1.6](#), Confidentiality of Information, now requires a lawyer to “make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.” [ABA Model Rules, 1.6\(c\)](#). A lawyer’s ethical obligations to maintain the confidentiality of a client’s data is tied to [Rule 1.1](#). Comment 16 to 2012 Amendments to ABA Model Rules of Professional Conduct (“A lawyer must act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision.”).

21st Century data privacy concerns are evident in the amendments to the Model Rules:

A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client’s information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

Comment 16 to 2012 Amendments to ABA Model Rules of Professional Conduct.

B. Litigation Methods.

A critical component of a document retention policy is a “document hold” or “litigation hold” procedure.² Once a company “reasonably anticipates” that a legal action or investigation is threatened, contemplated, or underway, the company must draft and disseminate a litigation hold letter to advise employees to preserve documents and suspend document destruction policies. When a legal action is “reasonably anticipated” is a difficult question for many companies. Does a trucking company have to issue a legal hold every time one of its drivers is involved in a fender bender? Probably not. If the motor vehicle collision results in serious injury or death, a legal hold letter should be disseminated. Does a company have to issue a legal hold every time it terminates an employee? Probably not. When the employee resigned and alleged mistreatment and discrimination, probably. A legal procedure or investigation can be reasonably anticipated when a corporation receives a notice of claim, an EEOC Notice of Charge of Discrimination, a complaint, a notice of the filing of an administrative proceeding, a demand letter from a lawyer or some other written or verbal communication that indicates that a suit will or has been filed. The nature of the proceeding will dictate the documents to be preserved, but the company should err on the inclusive side.

Several key elements apply to all litigation hold letters to ensure that employees preserve and do not destroy documents. The letter should be drafted and disseminated immediately after the corporation determines a triggering event has occurred. At the initial phase of the proceeding, the corporation should identify records custodians and advise them of the claim and the categories of documents that must be preserved. Immediacy is crucial because ESI, more so than paper documents, is often destroyed daily as part of automated document destruction policies and during the recycling of backup tapes. A company can face many sanctions—from an adverse inference to the striking of a pleading—if documents are destroyed, even inadvertently. Further, companies may compound the problem created when they fail to distribute a letter at the onset of the proceeding by failing to issue one later in the litigation; even a delinquent litigation hold letter will assist the company in meeting its document preservation and collection obligations.³

The company need not send a global litigation hold letter. Instead, employees who possess potentially relevant information and documents must receive it. Records custodians in Human Resources, Research and Development, Operations, Marketing, and Information Technology, will also need to receive litigation hold letters to the extent appropriate.

The letter's scope, tone, and author are important. The letter must explain that the duty to preserve records is important to the company's litigation position. It should also identify the parties, the relevant dates, where the action is pending, and should convey the serious nature and facts – preferably without too much legalese. The import of the letter is bolstered if the General Counsel signs the letter and copies the Chief Executive Officer.

The letter should expansively define the term “document” and the duties to preserve and not destroy must be explained. The document custodian must be told not to destroy documents, either under the document retention policy or otherwise, even if they believe the documents may hurt the company and they should be reminded of that periodically until the matter is concluded. They should also be told that the company could be hurt just as much (if not more) by obstruction-of-justice and spoliation-of-evidence charges arising out of the destruction of documents than it might be by preserving documents that may hurt the company.

Finally, the letter should instruct that the duty to preserve and collect is ongoing and document destruction policies should be suspended until further notice.⁴ Attorney supervision of document collection, especially ESI collection, is imperative because employee-only searches more often destroy responsive documents than preserve them.⁵ Management, with the assistance of IT personnel, should periodically follow up with the letter's recipients to ensure compliance with the employees' preservation duties and to answer any questions that may arise.

C. Practical Information System Policies and Practices.

A corporation's information system policies and practices protect and secure a company's data, instruct employees on the proper use of technology in the workplace, and provide a competitive advantage in the marketplace. Information technology (“IT”) departments develop the policies with the human resources, operations and legal departments. Like technology, information system policies are not static, and changes to technology require IT departments to review and revise the policies periodically to meet the business's needs.

Companies typically tailor information policies to their business but the following general categories exist:

- Acceptable use policy
- Password policy
- Backup policy
- Confidential data policy



- E-mail use policy
- Document retention policy
- Mobile device/personal device/bring your own device to work policy
- Remote access policy

“Acceptable Use” policies, which establish the acceptable uses of company-owned technology, set the tone for employee computer use in the workplace. The policy should apply to all devices the employee uses to conduct company business including company computers, smartphones, cameras, networking equipment, and software, and to all uses of the technology, such as e-mail, texting, and instant messaging. Employees retain certain rights and freedoms when using company-owned technology—using e-mail to engage in labor practices protected by the National Labor Relations Act and other federal and state laws—and the policy must advise them that despite these rights company technology must be used for business purposes only. The acceptable use policy can contain password or e-mail policies, or they can be stand-alone policies.

Some businesses are required by law to implement policies and practice. For example, medical professionals must devise practices consistent with the Health Insurance Portability and Accountability Act and financial institutions must implement procedures to comply with Sarbanes Oxley and the Gramm-Leach-Bliley Acts.

Recent hurricanes underscore a need for business continuity and disaster recovery plans. What happens when the lights go out? Where is the back-up data stored? Is it secured? How quickly can employees gain access to data and get back on-line. Disaster recovery plans cover these situations.

Bring Your Own Device (“BYOD”) policies are critical to companies that allow employees to utilize their personal mobile devices for work purposes. The policy should identify the employees/positions allowed to use their own device at work, the need for IT approval of the device and the device’s compatibility with the company’s IT systems as a condition precedent to use of the device. The IT Department must install virus protection software on the device, and that the employee bears the risk for lost data. The employer also should be sensitive to wage and hour issues if the employee is an hourly employee. Last, the employee should acknowledge the conditions of use through a signed user agreement.

A document retention/destruction policy outlines how long documents—both paper and electronically stored—are kept before they can be destroyed. Federal and state law requirements and business and litigation needs dictate how long certain types of documents, such as tax, human resources, insurance and benefits information,



construction drawings, customer contracts, settlement agreements, and deposition transcripts must be kept. Historical corporate documents, such as by-laws, articles of incorporations, and asset purchase agreements should be kept indefinitely. Consistency is key—follow the policy’s destruction deadlines to avoid claims that documents were destroyed during pending litigation.

D. Preparing for the Rule 26(f) or Initial Scheduling Conference.

The [Federal Rule 26\(f\)](#) conference and initial scheduling conference are counsel’s first (and most important) opportunities to impress upon opposing counsel and the court the scope and magnitude of e-discovery issues in the case. These opportunities should not be wasted. The plaintiff should outline the affirmative e-discovery sought from the employer—personnel files, employment records, document retention policies, names of records custodians—while the employer should explain the company’s document retention and production capabilities, and cost issues. Preparation for the [Rule 26\(f\)](#) conference cannot wait, and should start when the client retains counsel to pursue or defend the claim.

Counsel should not delay discussing e-discovery capability issues with the client because the federal rules impose strict discovery deadlines on counsel. [Rule 26\(f\)](#) is very specific—“the parties must confer *as soon as practicable*—and in any event at least 21 days before a scheduling conference is to be held or a scheduling order is due under [Rule 16\(b\)](#).” [FED. R. CIV. PROC. 26\(f\)\(1\)](#). An effective [Rule 26\(f\)](#) conference results from a counsel-client working relationship focused on understanding a client’s ESI capabilities, however limited they may be. A lawyer’s e-discovery pre-conference strategy should include the following:

- 1) Preparing for the initial conference means becoming educated on a client’s computer systems, document retrieval capabilities and retention policies. Counsel should meet or set aside time to discuss e-discovery issues with the client, even if lawyer and client initially do not think ESI will play a role in the case. Separate time must be set aside because the potential pitfalls of e-discovery, especially its costs, must be addressed before the issues arise. For plaintiffs’ counsel, the meeting may only concern the client’s personal computer, information stored on the work computer, and social media. However, the prevalence of smartphones, a plaintiff’s smartphone use, especially company-owned smartphones, should be discussed.
- 2) The defense lawyer will likely have a greater learning curve than plaintiff’s counsel to prepare for the conference given the size, nature and location of the employer’s ESI and records custodians; employer



defendants are naturally the logical target of electronic discovery requests. Typically, employers' counsel must explain the employer's electronic document capabilities at the initial scheduling conference, so the meeting should take place well before the conference and [Rule 26\(f\)](#) meet and confer.

3) In appropriate cases, lawyer and client should give immediate thought to assembling an e-discovery team. Often in-house counsel do not have the time or qualifications to be the front persons for outside counsel's investigation of the client's technology capabilities. Other company employees, such as the director of information technology or similar position, can facilitate the collection and production of ESI and explain the company's document retention policy, preservation protocols, databases, servers, computers (desk and laptop), back-up tapes, disaster protocols, social media, and personal devices such as smartphones, cameras, laptops etc. The team also will identify records custodians and implement a legal hold (if not already distributed) to the custodians to preserve records. Third-party IT team members, including a representative from the lawyer's firm's IT department, may have to be recruited to facilitate the lawyer's e-discovery learning curve and the ultimate production of documents; third-party IT consultants may take on a larger role for smaller clients that have no dedicated IT staff, or in cases involving large quantities of ESI.

4) The lawyer, whether plaintiff or defendant, must know the client. Not all cases and clients are created equal—not every employment lawsuit is against a Fortune 50 company. Not every defendant has sophisticated back-up systems, IT departments, databases, and document retention policies. The outside lawyer must be sensitive to these issues when working with the client. The lawyer should not discount a client's technology capabilities if they appear "primitive" compared to recent advances in technology and computer systems. Rather, this issue should be front and center to all e-discovery discussions at the "meet and confer" and initial scheduling conference. Outside counsel should be candid with opposing counsel and the court about the client's capability to respond to electronic discovery requests under [Federal Rule of Civil Procedure 34](#). Finally, aggressive plaintiffs' counsel will demand and pressure defendants at the conference on e-discovery



issues. Defense counsel must be prepared, and, if that means bringing an IT person to the conference or allowing a technology savvy associate to handle the e-discovery discussions then do so.

E. Preparing Requests and Responding to Discovery Requests Involving Electronic Data.

Depending on the case, e-discovery can be very expensive. Individual restrictive covenant and discrimination cases might be more paper intensive than a collective action under the FLSA, for example, which requires the production of electronically stored accounting and payroll records. No matter the case, certain factors govern how to prepare and respond to e-discovery requests.

The guiding principle to cost-effective e-discovery is to know the case before drafting the interrogatories or document requests. Fishing expeditions, long the hallmark of traditional paper discovery, are not tolerated for e-discovery requests. [FED. R. CIV. PROC. 34\(a\)\(1\)\(A\)](#) (document request must be drafted with “reasonably particularity”); [Mailhoit v. Home Depot, U.S.A., Inc., 285 F.R.D. 566, \(D. Cal. Sept. 7, 2012\)](#) (limits placed on social media document requests because defendant failed to show how information sought was “reasonably calculated to lead to the discovery of admissible evidence”).

With the amendment to [Rule 26\(b\)\(1\)](#), lawyers in federal court must draft discovery understanding that courts will balance the burden of e-discovery to make sure the requests are proportional to the case. In [Noble Roman’s, Inc. v. Hattenhaur Distributing Company, 314 F.R.D. 304 \(S.D. Ind. 2016\)](#), the court ruled that defendant’s “wide-ranging” discovery requests, including seeking documents about every aspect of the plaintiff’s business operations, was nothing more than a fishing expedition and “outside the proper bounds of discovery.” [Id. at 311](#). The court noted that the proportionality requirement of [Rule 26\(b\)\(1\)](#) protects litigants from burdensome and far-reaching discovery, describing defendant’s discovery requests as “discovery run amok.” [Id. at 311](#). The decision serves as a guide to drafting discovery requests:


Hattenhauer beats the drum of “relevancy.” It asserts that all of its deposition topics and document requests are “relevant.” That’s not good enough. Hattenhauer never attempts to demonstrate that the discovery is in any way proportional to the needs of this case, considering such things as the amount in controversy, the importance of the information in resolving contested issues, whether the burden of the discovery outweighs its likely benefits, whether the information can be obtained

from other and more convenient sources, or whether the information is cumulative to other discovery Hattenhauer has obtained.

[Id. at 311](#). The discovery requests must be specifically tailored to the facts that are not only relevant to the dispute but proportionally relevant to the dispute. \$100,000 in e-discovery productions expenses should not be spent on a \$50,000 case. See [id.](#) Amended [26\(b\)\(1\)](#) reinforces court management over discovery so counsel should follow the dictates of the amendment when drafting e-discovery requests. If counsel knows the case before drafting discovery, it will be easier to tailor specific requests that avoid costly fishing expeditions.

“Knowledge is power.” A lawyer must know where the documents are to draft concise and specific e-discovery requests. Relying on the client (both plaintiff and defendant) or former employees allows counsel to understand the computer systems used, storage locations, and destruction/retention policies. Further, with a working knowledge of the client’s computer systems, counsel can better manage any e-discovery issues that may arise with the court and opposing counsel.

Responding to e-discovery requests is no easy task and requires a team effort. Just like preparing for the initial conferences, counsel must communicate with client and client personnel to understand the systems, documents created and storage locations, how information is preserved, and the potential cost to produce it. Those factors all impact how counsel can respond to e-discovery requests.

When drafting responses remember that the Federal Rules demand specificity—so challenge those requests that are not and seek a protective order if necessary. Further, request follow-up conferences with the magistrate if e-discovery issues become unmanageable or unduly burdensome. E-discovery can overwhelm but it is manageable. 

Endnotes

- 1 The states are: Arkansas, Arizona, Connecticut, Delaware, Idaho, Illinois, Iowa, Kansas, Massachusetts, Minnesota, New Hampshire, New Mexico, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Utah, Virginia, Washington, West Virginia, Wisconsin and Wyoming.
- 2 A portion of this section is an excerpt from FDLI Monograph Series, *The New Reality of Sales Force Behavior and Management*, Vol. 2, Number 6 (June 2011), and is used with permission.
- 3 See *The Pension Committee of the University of Montreal Pension Plan, v. Banc of America Securities, LLC*, 685 F. Supp.2d 456, 476-477, 489 (S.D.N.Y. 2010).
- 4 *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004) (*Zubulake V*) (issuance of litigation hold letter is the beginning, not the end, of the company’s e-discovery duties)
- 5 See *Pension Committee*, 685 F. Supp.2d at 471.