

Ethics and the Discovery of Electronically Stored Information

By James D. Walker Jr.¹
and
Amber Nickell²

Introduction

Under general principles of legal ethics, attorneys must be competent to perform the legal work required of them.³ They must communicate sufficiently so their clients can “make informed decisions regarding the representation.”⁴ They must expedite litigation⁵ and refrain from obstructing the opponent’s access to evidence.⁶ An attorney who fails to understand the client’s use of electronically stored information (“ESI”) or ESI in general cannot be competent to deal with the discovery issues ESI raises, cannot adequately explain the intersection between ESI and discovery to the client, and cannot deal with ESI in a manner that ensure expeditious litigation and cooperation with the opponent.

As early as 1996, the Rules Committee recognized the unique problems raised by ESI in the discovery process—such as significantly greater volumes of information; a dynamic nature, in which the information can be easily changed, overwritten, or deleted, even without the user’s knowledge; and native formats that can only be read by the systems that created them.⁷ In 2000, the committee began the process of revising the Federal Rules of Civil Procedure to address the

1 Bankruptcy judge, Middle District of Georgia.

2 Law Clerk to Judge Walker.

3 Model Rule of Professional Conduct 1.1.

4 Id. 1.4(b).

5 Id. 3.2.

6 Id. 3.4(a).

7 Summary of the Report of the Judicial Conference Committee on Rules of Practice and Procedure, at p.22-3 (September 2005).

issues raised by ESI.⁸ The product of its work can be found in the amendments to the Rules effective December 1, 2006, including Rules 16, 26, 33, 34, 37, and 45.⁹ In addition, Congress enacted corresponding Rule of Evidence 502, effective September 9, 2008, to address concerns about waiver of attorney-client and work-product privilege when dealing with discovery of ESI.

Initial ESI Considerations

Communicate Early to Facilitate Compliance With the Rules

Although attorneys and courts were dealing with the implications of ESI long before formal rules were adopted,¹⁰ the scope of the Rules amendments implicitly encourages, even requires, discussion and development of ESI policies at the outset of the representation in two ways. First, ESI considerations will arise early during discovery, leaving little time for an uninformed attorney to get up to speed. For example, under Rules 16 and 26, the attorney must be prepared to discuss and formulate a plan with the opposing party that addresses such items as the location and content of ESI, preservation of ESI, and the form of its production. Second, having an ESI management policy in place prior to litigation may provide a safe harbor from sanctions related to failure to produce ESI due to its loss or destruction, pursuant to Rule 37(e). Consequently, waiting until the onset of litigation to discuss ESI with the client may make compliance with the Rules difficult, if not impossible. On the other hand, advance preparation

⁸ Id. at 22.

⁹ These Rules are made applicable to adversary proceedings in bankruptcy by Federal Rules of Bankruptcy Procedure 7016, 7026, 7033, 7034, 7037, and 9016.

¹⁰ See Zublake v. UBS Warburg LLC, 217 F.R.D. 309, 311 (S.D.N.Y. 2003) (“As individuals and corporations increasingly do business electronically—using computers to create and store documents, make deals, and exchange e-mails—the universe of discoverable material has expanded exponentially.”) (footnotes omitted).

“can greatly ease the burdens and risk of inaccuracy inherent in efforts to prepare of initial disclosures and meet and confer sessions once litigations begins.”¹¹

Cast a Broad Net

The Rules anticipate the attorney has a thorough understanding of all aspects of the client’s ESI, from its creation, to its content, to its storage, to its destruction. To acquire such knowledge, discussions with the client should, at a minimum, cover four areas: what, where, who, and how.

What: What type of information and records are created and stored electronically? This may include e-mails, text messages, instant messages, facsimilies, voice mail, and computer generated documents such as spreadsheets and memos.¹² With respect to application of the Rules, this information is important because parties are required to provide, as part of the initial disclosures, “a description by category” of relevant ESI,¹³ in addition to the more general provision that parties may obtain any relevant, nonprivileged information.¹⁴

Where: Where is the information created and stored? This may include computer hard drives, flash drives, backup tapes, and PDA devices.¹⁵ The attorney should also determine what types of software are used to create the ESI.¹⁶ Not only must the party disclose the location of relevant ESI as part of its initial disclosures,¹⁷ it also must produce ESI unless it is “not

¹¹ The Sedona Principles, 2d ed., Best Practices, Recommendations and Principles for Addressing Electronic Document Production, at p.30 (The Sedona Conference Working Group Series 2007).

¹² Todd L. Newton, E-Discovery and Record Retention: When Two Worlds Collide, 43 Ar. Law. 16, 18 (Spring 2008); Andrew T. Wampler, Ethics and Management of E-Discovery, 44 Tenn. B.J. 22, 23 (October 2008).

¹³ Fed. R. Civ. P. 26(a)(1)(A)(ii).

¹⁴ Id. 26(b)(1).

¹⁵ Newton, supra note 12, at 18.

¹⁶ Wampler, supra note 12, at 24.

¹⁷ Id. 26(a)(1)(A)(ii).

reasonably accessible because of undue burden or cost.”¹⁸ For example, if the ESI “is retained only on backup tapes that are kept for business continuity purposes, then there may be an argument that such information is not reasonably accessible and does not have to be initially produced.”¹⁹ Similarly, data that can be read only by obsolete systems or deleted and fragmented data that can only be recovered by forensic examination may be deemed inaccessible.²⁰

Determining the accessibility of ESI “does not solely depend on the technology required to access that information, but is more closely related to the costs and burdens involved in accessing and retrieving the information.”²¹ And, even reasonably inaccessible ESI may be subject to production “if the requesting party shows good cause.”²² Factors courts may consider in the good-cause inquiry include the following:

- (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.²³

It should go without saying that a “party may not deliberately make information inaccessible for the sole purpose of avoiding litigation discovery requests specific to a known

¹⁸ Id. 26(b)(2)(B). Nevertheless, the existence of inaccessible data must be disclosed if “the producing party believes in good faith it may contain relevant, non-duplicative information.” Sedona Principles, supra note 10, at 18.

¹⁹ Newton, supra note 12, at 18.

²⁰ Sedona Principles, supra note 11, at 18.

²¹ Id. at 46.

²² Fed. R. Civ. P. 26(b)(2)(B).

²³ Id. comment to 2006 amendments.

case.”²⁴ For example, in Disability Rights Council v. Washington Metropolitan Transit Authority,²⁵ 242 F.R.D. 139 (D.D.C. 2007), the defendant failed to stop routine purging of email until more than two years after the complaint was filed. The court required the defendant to produce the backup tapes for those emails, which were not reasonably accessible, stating it could not “permit a party who has failed to preserve accessible information without cause to then complain about the inaccessibility of the only electronically stored information that remains.”²⁶ This case also underscores the importance of the litigation hold, discussed later in this article.

Who: Who creates and uses the ESI? This information is important because “it may be the only way to know all the types of records, paper and electronic, that are being kept and where they are located.”²⁷ In other words, this question is necessary to ensure complete answers to the “what” and “where” inquiries. In addition, identify those responsible for preserving and producing ESI. They will be necessary participants in creating a practical ESI management policy.²⁸ Finally, find out if the client either outsources any of its ESI functions or shares any of its ESI with third parties, which will be useful in later knowing who should be notified of a litigation hold.²⁹ Consider providing by contract for the possibility of involving such third parties in the ESI discovery process.³⁰

How: How is the ESI managed? Once the “what,” “where,” and “who” questions are answered, the attorney and client can effectively evaluate an existing ESI management system or create a new one. Such a system should provide “policies and procedures for preserving and

24 Sedona Principles, supra note 11, at 46.

25 242 F.R.D. 139 (D.D.C. 2007).

26 Id. at 147.

27 Wampler, supra note 12, at 40.

28 Id.

29 Sedona Principles, supra note 11, at 48.

30 Id.

producing potentially relevant information and establish[] processes to identify, locate, preserve, retrieve, and produce information that may be relevant or required for initial mandatory disclosures.”³¹ Keep in mind a generic or one-size-fits-all system will not suffice.³² It should be individualized, taking into account “the business, regulatory, tax, information management, and infrastructure needs of the organization.”³³ The system should address retention of any electronically created or stored information and electronic communications, and it should address back up media.³⁴ This will “ensure that pertinent records are being kept so long as there is a business need or legal obligation to do so.”³⁵ Furthermore, the system should include a routine destruction policy, “which will allow for some protections under the Safe Harbor Provision of the Rules.”³⁶ And, the system should provide procedures for imposing a litigation hold, including identification of those responsible for implementing the hold.³⁷

ESI Management During Litigation

Litigation Hold

Once litigation is imminent or initiated, the attorney and client will have two primary concerns with regard to ESI. First they must impose a litigation hold to preserve evidence. Second they must develop a plan in conjunction with the opposing party for production of the ESI. The litigation hold is an essential tool for complying with the duty to preserve evidence, the

31 Id. at 30.

32 Newton, supra note 12, at 39.

33 Sedona Principles, supra note 11, at 12.

34 Id.

35 Newton, supra note 12, at 40.

36 Wampler, supra note 12, at 24.

37 Id.

scope of which should be defined “as soon as practicable after [it] arises.”³⁸ Generally, the duty to preserve extends to what the party “knows or reasonably should know is relevant to the action.”³⁹ It attaches when litigation is reasonably anticipated.⁴⁰ At that time, the defendant “must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’ to ensure the preservation of relevant documents.”⁴¹ Failure to comply with the duty to preserve may result in significant sanctions, including monetary sanctions, limitation on witness examination, adverse inference jury instructions, adverse findings against the sanctioned party, or judgment against the sanctioned party.⁴²

To initiate a litigation hold, send a hold letter instructing the client to “freeze ... the destruction or alteration of ESI.”⁴³ The hold should cover key employees, likely sources of relevant ESI, and the availability of ESI from other sources.⁴⁴ But, it “should not require the complete suspension of normal document management policies, including the routine destruction and deletion of records.”⁴⁵ Be sure the person responsible for implementing the hold receives a copy of the letter. “It is generally not sufficient to send it solely to the client’s contact person who is managing the litigation.”⁴⁶ While the contents of the hold letter need not be overly specific, listing every piece of data to preserve, it should “describe the types of information that

38 Sedona Principles, *supra* note 11, at 31.

39 Douglas L. Rogers, A Search for Balance in the Discovery of ESI Since December 1, 2006, 14 Rich J.L. & Tech. 8, at *16 (Spring 2008) (citing *Benton v. Dlorah, Inc.*, No. 06-cv-2488-KHV, 2007 WL 3231431, at *4 (D. Kan. Oct. 30, 2007)).

40 *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).

41 *Id.* at 218. See also *Doe v. Norwalk Comm. Coll.*, 248 F.R.D. 372, 377 (D. Conn. 2007).

42 Rogers, *supra* note 38, at *6 (citations omitted).

43 Wampler, *supra* note 12, at 24.

44 Rogers, *supra* note 38, at *10 (citing *In re NTL, Inc. Sec. Litig.*, 244 F.R.D. 179 (2007)).

45 Sedona Principles, *supra* note 11, at 32.

46 Wampler, *supra* note 12, at 24.

must be preserved with enough detail to allow the recipient to implement the hold.”⁴⁷ A similar letter can be sent to the opposing party to put it on notice of its “obligation not to alter or destroy” evidence.⁴⁸

Compliance with a pre-existing ESI management plan coupled with a properly implemented litigation hold can protect a party against spoliation claims for failure to produce lost ESI. Under Rule 37(e), “[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of a electronic information system.”⁴⁹

Generally, sanctions for spoliation depend on culpability and prejudice, and the issue of good faith plays a role in evaluating culpability.⁵⁰ When ESI is lost, courts will consider whether the party took steps to preserve the data, notwithstanding the loss. Evidence that the loss of ESI was intended to prevent its discovery will create a stronger case for spoliation sanctions.⁵¹ However, even if the loss is negligent rather than intentional and it results in prejudice to the requesting party, “the court may nevertheless order remedial measures designed to put parties in roughly the [same] position they would have been [in] but for the negligence of the responding party.”⁵²

Furthermore, the safe harbor as to ESI destroyed by a routine destruction policy only applies to destruction that occurs before the duty to preserve arises. “Once a party reasonably determines that electronically stored information in its custody or control may be relevant to pending or reasonably foreseeable litigation, the party should take reasonable steps to preserve

47 Sedona Principles, supra note 11, at 32.

48 Wampler, supra note 12, at 24.

49 Fed. R. Civ. P. 37(e).

50 Sedona Principles, supra note 11, at 71.

51 Id.

that electronically stored information, even if its records management programs calls for its routine destruction.”⁵³ For example, in Doe v. Norwalk Community College,⁵⁴ the court stated “in order to take advantage of the good faith exception, a party needs to act affirmatively to prevent the [routine ESI management] system from destroying or altering information, even if such destruction would occur in the regular course of business.”⁵⁵ In Doe, the court found the defendant had no routine system in place for ESI management and it failed to suspend destruction of ESI during the pendency of the case, which resulted in the loss of relevant evidence.⁵⁶ The court ordered an adverse jury instruction as to the destroyed evidence and awarded costs to the plaintiff.⁵⁷

Factors in the good-faith inquiry may include the following:

- (a) was there a standard litigation hold process and was it followed?
- (b) did the party adequately communicate litigation hold instructions to employees?
- (c) did the party periodically distribute litigation hold reminders?
- (d) did the party adequately investigate and identify the locations that were reasonably likely to contain unique and relevant electronically stored information?
- (e) has the party been cooperative and forthcoming in Rule 26(f) and Rule 16(b) discussions?
- (f) has the party been reasonable and forthcoming in written discovery responses and depositions?
- (g) did the party take steps to secure relevant, unique electronically stored information that would otherwise be overwritten or deleted by automatic processes?
- (h) did the party take reasonable steps to ascertain whether orphaned or legacy data contain relevant information?
- and (i) was the electronic system designed and implemented solely with the intent of meeting business and technical needs or with the intent of thwarting discovery?⁵⁸

52

Id.

53

Id. at 73.

54

248 F.R.D. 372 (D. Conn. 2007).

55

Id. at 378.

56

Id.

57

Id. at 381.

58

Sedona Principles, supra note 11, at 72.

Because the question of good faith is fact-intensive and different courts may consider different factors, the safest approach for a party may be to “quickly and conscientiously determine what reasonable preservation steps it will take and then notify the other party of its conclusions.”⁵⁹ If the opposing party objects, the court can resolve the dispute, effectively preventing a spoliation issue arising months or years into the litigation.⁶⁰

Discovery Plan

Pursuant to Rule 26(f)(3), the parties’ discovery plan must contemplate “any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced[.]” Based on initial discussions with the client, the attorney should already have an inventory of the client’s ESI (e.g., type and location of the records, creators and users of the records, and impact of ESI management system on those records). The attorney should try to obtain the same type of inventory from the opposing party.⁶¹ Having such information from both sides allows the attorney to make an educated and reasonable ESI production request.

A reasonable request is often a narrow request. Thus, the requesting party should “to the greatest extent practicable, clearly and specifically indicate the types of electronic information it seeks.”⁶² Instead of requesting production of broad categories, such as all email, “the request should target particular electronically stored information that the requesting party contends is

59 Rogers, supra note 38, at 47.

60 Id.

61 Wamper, supra note 12, at 24.

62 Sedona Principles, supra note 11, at 25.

important to resolve the case.”⁶³ This reduces the possibility of objections requiring judicial intervention that may be created by setting forth a burdensome blanket request.⁶⁴

Rule 34(b)(1)(C) provides that the request for ESI “may specify the form or forms” in which it should be produced.”⁶⁵ When deciding the form of the ESI to request, keep in mind that asking for production of documents as an image file—such as a pdf—will exclude any metadata contained in the native file format such as the formulas used in producing a spreadsheet.⁶⁶ Of course, the production of metadata is, itself, a separate consideration that should be discussed by the parties. In addition to the need (or not) for metadata, other considerations as to form of production for the requesting party include: (1) which forms will most likely yield relevant evidence; (2) which forms provide reasonably accessible information; and (3) which forms are the most usable and manageable.⁶⁷

Producing parties also play a role in agreeing to the form of production. They should take into account:

- (a) the relative risks of inadvertent production of confidential, privileged, and work product information associated with different forms of production;
- (b) difficulties in redaction, tracking, and use of native files;
- (c) whether alternative (e.g., ‘nonnative’) forms of production provide sufficient usability ... such that the producing and requesting parties have the same access to functionality; and
- (d) the relative costs and burdens with respect to the proposed forms of production[.]⁶⁸

Metadata and forms of production are only two of the ESI issues parties must address in the early stages of the litigation. They should also try to resolve the following:

63 Id.

64 Id.

65 Fed. R. Civ. P. 34(b)(1)(C).

66 Sedona Principles, supra note 11, at 52.

67 Id. at 63.

68 Id.

- (1) which data sources which will be subject to preservation and discovery;
- (2) whether to limit discovery to ESI created during a particular time frame;
- (3) which people within or outside the organization are likely have relevant ESI
- (4) whether software necessary to read ESI will be provided, perhaps by a limited license;
- (5) whether any relevant information is reasonably inaccessible;
- (6) whether specific search terms will be used to reduce the volume of information produced and what those search terms will be;
- (7) which versions of documents will be produced, such as final drafts only; and
- (8) how to deal with inadvertent production of privileged information.⁶⁹

Throughout not only these preliminary steps, but also during the collection and production of ESI, it is useful to thoroughly document the process, which will “enable an organization to respond to challenges—even those made years later—to the collection process, to avoid overlooking electronically stored information that should be collected, and to avoid collecting electronically stored information that is neither relevant nor responsive to the matter at hand.”⁷⁰ These steps can help the attorney comply with ethical obligations to “provide effective representation and ensure that proper information is both obtained and produced, while keeping the case in proportion to its issues.”⁷¹

Privilege Issues With ESI

⁶⁹ Id. at 21; Wampler, supra note 12, at 25-26.

⁷⁰ Id. at 40.

⁷¹ Wampler, supra note 12, at 26.

Because producing ESI often requires reviewing huge quantities of data, the parties face an increased risk of inadvertently producing privileged information.⁷² However, common sense and reference to the Rules amendments can alleviate the problems created by this situation. First, take an active role in any privilege and relevance review.⁷³ The client acting alone probably cannot identify all privileged information. Second, under the Rules the parties can agree on a process for dealing with waiver and privilege claims, and such an agreement can be memorialized in the scheduling order.⁷⁴

Nonwaiver agreements between parties often include a clawback provision, “allow[ing] the producing party to ‘claw back’ or ‘undo’ the production” of privileged information.⁷⁵ In fact, Rule 26(b)(5) sets forth what can be described as a default clawback procedure to be used in the absence of a separate agreement by the parties. It allows the producing party to make a claim of privilege as to information already produced and prevents the responding party from using the disputed information until the court resolves the claim.⁷⁶ The parties may also consider a “quick peek” agreement, under which the opposing party sees the documents and ESI prior to the privilege review.⁷⁷ “[I]f the requesting party selects a document that appears to be privileged, the producing party can identify the document as privileged and withdraw it from production without having waived any privilege.”⁷⁸ A quick peek agreement may raise ethical issues not associated with clawback arrangements. Specifically, it may run afoul of the attorney’s duty to

⁷² Fed. R. Civ. P. 26, comment, 2006 amendments.

⁷³ Wampler, *supra* note 12, at 25.

⁷⁴ Fed. R. Civ. P. 16(b)(3)(B)(iv); 26(f)(3)(D).

⁷⁵ Sedona Principles, *supra* note 11, at 51.

⁷⁶ Fed. R. Civ. P. 26(b)(5)(B).

⁷⁷ Sedona Principles, *supra* note 11, at 54.

⁷⁸ *Id.*

protect client confidences, or it may violate privacy rights and the client’s agreements with employees or third parties.⁷⁹

One thing the Rules of Procedure do not address is whether inadvertent disclosure of privileged information can lead to waiver of the privilege. Rule of Evidence 502, which became effective in September of 2008, fills the gap in some respects. It provides in a federal proceeding “an inadvertent disclosure of privileged information does not constitute a waiver as long as the holder took reasonable steps to prevent disclosure and acted promptly to retrieve the mistakenly disclosed information.”⁸⁰ Thus, to take advantage of the new Rule of Evidence, the parties should fully exploit the confidentiality agreements and procedures allowed under the Rules of Procedure to ensure they take all the necessary precautions against disclosure.

Final Thoughts

The key principles of this article easily can be distilled to a few sentences. At the outset of representation, learn as much as possible about the client’s ESI, including what it is, where and how it is stored, and who creates it. Make sure the client has a retention and destruction policy in place and that it carries out the policy consistently. Once litigation is imminent, invoke a litigation hold and prevent any destruction (even routine destruction) of possibly relevant information. Be prepared for early discussions of the details of ESI production with opposing counsel, including a description of content and location (including accessibility) of relevant ESI, the form of its production, and any agreements for protecting confidentiality. These steps should help expedite and simplify a potentially laborious process.

⁷⁹

Id.

⁸⁰

Fed. R. Evid. 502, Sen. Rep. No. 110-264, at 3 (2008).