

10

E-Discovery (and Ethics) Tips for Lawyers

BY LYNDA C. SHELY & DAVID DEGNAN

LYNDA C. SHELY is a principal at The Shely Firm, PC, Scottsdale. **DAVID DEGNAN** is an attorney at Alvarez & Gilbert, PLLC, Scottsdale.

1 The Duty to Preserve Information Begins When Litigation is “Reasonably Anticipated”

The first basic step in understanding “e-discovery” obligations is knowing when that duty to preserve relevant evidence begins. According to case law, it begins when litigation is “reasonably anticipated.”

For example, indirect threats or comments about litigation are not enough to trigger the duty to preserve. On the other hand, a formal demand letter with instructions to issue a litigation hold letter or notice of a formal investigation are likely enough to put a party on notice of pending litigation, and the client’s duty to preserve, before the complaint is filed.

ETHICS TIP: All lawyers representing a client who may be headed toward “reasonably anticipated” litigation need to understand the obligation to preserve possible evidence (Ethical Rule 3.4). That means training all lawyers and all staff, not just the litigation section, that nothing may be deleted or destroyed once there is a pretty darn good chance of litigation on some matter related to the client. Lawyers should err on the side of preserving possible evidence rather than risking the chance that maybe the opposing party really didn’t mean they were going to sue.

2 Warn Clients to Suspend Document-Retention Programs and Place a Litigation Hold on Documents Once Litigation is Reasonably Anticipated

A document-retention policy is a formal (or informal) set of guidelines that explains what documents should be retained and for how long. When drafting these policies, counsel must consider a document’s value in terms of statutory obligations, regulatory scheme, or some other business purpose.

If a party properly follows its document-retention policy and destroys an otherwise hot document before litigation is anticipated, then the policy acts as a shield from spoliation. *See* ARIZ.R.CIV.P. 37(g). However, once litigation is reasonably anticipated, the document-destruction policy must be suspended, relevant evidence must be preserved, and attorneys must oversee the preservation and then production of tangible and electronic documents.

ETHICS TIP: Every law firm needs to have a records-retention policy that must comply with ER 1.15 and ER 1.16 because clients own their “files,” and records in the lawyer’s possession not only are client property but may be subject to discovery. Comment [9] to ER 1.16 defines the “file” as pretty much everything—including work product, research, pleadings, correspondence, notes and email. Arizona Ethics

The Arizona Rules of Civil Procedure permit liberal discovery into “any matter, not privileged, which is relevant to the subject matter involved in the pending action.” ARIZ.R.CIV.P. 26(b)(1)(A). That includes electronically stored information on such equipment as computers, smart phones, and fax and copy machines.

All lawyers, not just trial lawyers, must understand how to preserve and then produce electronic information that is in its client’s (and possibly the law firm’s) possession, custody and control. This article provides 10 electronic discovery tips—and corresponding ethics advice for both discovery and ethics compliance.

JAMES TREW © SHUTTERSTOCK.COM



Opinion 08-02 requires that lawyers “tender” the entire file to the client at the conclusion of the representation. So even if the file is not discoverable, lawyers still must provide the client with their file—and that may include electronic records.

3 **Lawyers Must Oversee the Preservation of Electronic Discovery**

Counsel must ensure that he or she preserves relevant evidence for litigation. For example, counsel likely would not sue for an alleged product defect if his or her client threw away the defective product. Similarly, counsel cannot let computer evidence be overwritten or deleted if that information may be relevant to the dispute.

In short, counsel must take steps to ensure that the proper documents are preserved. This requires counsel to do the following: identify relevant individuals who may have relevant information, send out litigation hold notices, distribute acknowledgment forms to relevant individuals, audit the client’s litigation hold efforts, safeguard the client’s data, and meet with opposing counsel to define and to limit the scope of preservation.

ETHICS TIP: Lawyers are responsible for supervising staff—including independent contractors or consultants. This means assuring not just their competence to undertake the review of electronically stored information, but also that they maintain the confidentiality of any client information they view, including securing work areas and having appropriate back-up systems, firewalls, anti-virus protection, and sufficient computer security systems. The lawyer could be responsible for their negligence and definitely will be responsible if the independent contractors misuse or destroy possible evidence. Contracts with independent contractors should include appropriate security, confidentiality and competence provisions.

4 **Computer and Paper Data Must be Collected in a Manner That Ensures Admissibility**

Evidence must be preserved in a manner that ensures trustworthiness, reliability and admissibility. In the paper world, one frequently could tell when a document was

altered. However, computer files are more susceptible to be modified, which should be obvious to anyone that has edited a Microsoft Word document or taken the “red eye” out of a photo. Therefore, to ensure reliability, sophisticated counsel might seek to record the chain of custody and ensure that the electronic documents are secure and unaltered.

ETHICS TIP: Just as electronically stored information must be protected to assure admissibility, client files must be secured because they are client property—whether they are paper files or electronic files. For instance, do not delete client-related emails, because they are communications that are part of the client “file.” Lawyers should have an electronic records filing system that assures that the emails can be located and provided to the client at the end of the representation, and train staff to use a firm-wide consistent filing protocol such as creating subfolders by client or attaching emails to the client’s contact information in your case-management software.

5 **Collected Data Must Be Produced in a Reasonably Usable Form**

Rule 34 requires that counsel produce documents in an organized and usable form. To do that, counsel may produce documents in native, PDF, or TIFF format. But when users convert documents from Microsoft Word to PDF format, for example, they are creating a new document and are stripping the metadata from the original file. This strategy is important to use when sending client correspondence to the opposing counsel; however, this tactic should be used with caution when producing discoverable information to the other party. Wise counsel will reach an agreement with opposing counsel on the preferred form of production before spending the money to convert and then produce large quantities of documents.

ETHICS TIP: In addition to law firms maintaining client “files,” remember that the discovery obtained from the opposing party in a matter also is part of the client’s file, which means not only storing the firm’s records but also all paper and electronic dis-

covery from the opposing party. Given that Arizona Ethics Opinion 08-02 encourages lawyers to “tender” the entire client file to the client at the conclusion of the representation, this would mean also giving the client all the opposing party’s discovery. If the client does not want to receive their entire file at the conclusion of a representation, then the firm will have an obligation to preserve the file for at least three years, which is the time in Arizona that it takes for property to become abandoned. (Note: Longer retention periods may apply for certain criminal defense, estate planning and juvenile matters).

If, however, the client accepts their entire file at the end of the case, the firm may decide to retain the firm’s copy for a shorter period of time. Note that while the statute of limitations for a malpractice claim may be two years, there is no statute of limitations on a Bar complaint. Also check the firm’s malpractice policy for file-retention requirements.

6 **Metadata is Discoverable—Kind Of**

Counsel should be aware of the following three standard types of metadata that may be relevant to his or her case: substantive metadata, system metadata, and embedded metadata.

Substantive metadata “reflects substantive changes of the user” and includes “modifications to a document, such as prior edits or editorial comments, and data that instructs a computer how to display fonts and spacing of documents.”

System metadata “reflects information created by the user or the organization’s information management system” and includes the “author, the date and time and creation, and the date a document was modified.”

Embedded metadata includes “spreadsheet formulas, hidden columns, externally or internally linked files (such as sound files), hyperlinks, references or fields, and database information.”¹

ETHICS TIP: Though metadata may be discoverable, that does not mean that lawyers ethically may view metadata inadvertently left in documents sent to them by opposing parties/counsel. Arizona Ethics Opinion 07-03 prohibits the review of metadata in documents received from other people that is not intended to be reviewed (i.e., opposing parties/counsel). Lawyers also have an affirmative duty to



be competent and “scrub” metadata from documents sent to other lawyers/parties to avoid the inadvertent disclosure of confidential information. Ethical Rule 4.4(b) requires that lawyers who receive confidential information that may have been sent inadvertently to notify the sender and maintain the status quo for a reasonable period of time to permit the sender to take protective action.

7 Beware of the “Cloud”

This doesn’t mean monsoon storms. Companies often seek to store information on an Internet server, also known as “in the cloud.” Cloud computing has several advantages, including increased space, reduced need for storage and warehouse staffing, and increased organization of the client’s information. However, cloud computing has several risks, as well.

The chief risk is that no one really knows where the data is located, whether European Privacy laws apply, or if someone else is looking at their data. As a result, wise counsel will (attempt to) negotiate with the cloud provider to draft and revise important terms, decide on a choice of law provision, confirm data security requirements and protocols, and describe notice requirements in the event that someone wishes to access your data (i.e., the government pursuant to a warrant).

ETHICS TIP: Wherever a lawyer stores client documents—in file cabinets, boxes in a storage facility, or electronically on a shared Internet source—the lawyer is responsible for assuring the security of the documents and that they can be retrieved.

Arizona Ethics Opinion 07-02 permits electronic storage of client “files” as long as: (1) the document integrity is not compromised by the electronic storage; (2) the storage is secure; and (3) the client consents to and has the ability to “read” the electronically stored documents. For instance, if a client does not know what you’re talking about when you mention a thumb drive, jump drive or CD, the lawyer probably will need to provide the client with paper copies of documents.

Warning: Many large corporations do not permit their law firms to store information remotely (aka “the cloud”) because of security concerns. Therefore, consider two cautions: (1) always ask client permission (in

the fee agreement) if the firm wants to use cloud storage; and (2) confirm what security measures the “cloud” provider uses, including: how the provider responds to subpoenas for *your* firm files, where its server is physically located (country), what background checks it does for its own employees, and what happens to your information if it goes out of business.

8 Social Media Is a Good and Bad Thing

Social media has grown significantly in the last seven years. Companies such as Facebook, LinkedIn, WordPress and others are becoming commonplace in our society. Indeed, lawyers and clients are using these forums to connect, network and interface with other potential clients and customers.

However, social media also may provide a vehicle to distract employees, admit liability to crimes, or provide circumstantial evidence that may be relevant to litigation. Therefore, counsel should properly instruct their clients to use social media and define policies and procedures for using social media within the workplace.

ETHICS TIP: Every law firm should have a social media policy that discusses at least: (1) how lawyers and staff may use social media as a marketing tool for the firm (only using the firm name with management approval), (2) how all lawyers and staff are prohibited from discussing client matters on the Internet—whether at work or at home—unless authorized to do so to carry out the representation, and (3) how clients should be reminded not to discuss their legal matter on the Internet.

Additional cautions include avoiding spoliation charges by warning clients not to delete or remove social media information if litigation is anticipated, and not “friending” or linking to opposing parties, witnesses or judges assigned to a case.

9 E-Discovery Is Expensive


There is no simpler way put it: E-discovery is expensive. According to a recent article, the cost to process 100 gigabytes of information is between \$75,000 and \$180,000. Moreover, the cost to hire outside contract reviewers to review each document is between \$7,000 and \$284,375 depending

on the circumstance.² Given the costs, counsel must take steps to reduce the volume of information, whenever possible. To do this, counsel must understand the legal elements of its case to properly sample, to reach agreements with opposing counsel about the scope of preservation, and to work with vendors to focus the search as much as possible on relevant evidence in a manner that produces the smallest number of false positive documents.

ETHICS TIP: Talk to clients about the expense before diving into electronic discovery and preferably even before filing suit. Clients need to have a clear understanding of the expense associated with e-discovery. Then meet with opposing counsel to work out a fair and reasonable discovery process that is consistent with the client’s objectives that is cost-effective. Provide clients with updates throughout discovery regarding unforeseen developments that could affect expenses.

10 E-Discovery in Criminal Cases Is Evolving

Courts have not embraced criminal e-discovery with the same fervor as their civil counterparts. However, criminal attorneys should not ignore its obligation to preserve relevant evidence that may be stored on a computer. In *Brady v. Maryland*, the court held that the prosecution must disclose material evidence to the defendant. Since *Brady*, in *United States v. Dollar*,³ a U.S. District Court dismissed the government’s claim for failing to meet its *Brady* obligations and producing exculpatory evidence. As a result, counsel should not overlook an important source of relevant evidence that may implicate or exonerate its client.

ETHICS TIP: Criminal defense lawyers should not assume that they are “immune” from e-discovery and should consider how it could assist their case and include ESI as part of their discovery requests. 

endnotes

1. *Aguilar v. ICE*, 55 F.R.D. 350, 353-355 (S.D.N.Y. 2008).
2. See David Degnan, *Accounting for the Costs of Electronic Discovery*, 12 MINN. J. L. SCI. & TECH. 151, 169 (2011).
3. 25 F. Supp. 2d 1320, 1322-23 (N. D. Ala. 1998).