CAUTION! Electronic

Picture yourself in the courtroom waiting for the judge. You sit at counsel table next to your client and your partner. The gavels raps, and the judge assumes the bench.

She is visibly irked. Directing her gaze first to you, then to her papers, the judge begins to speak. The tone of her voice portends doom, for someone. You begin to worry, "Is it me?"

You cannot make out everything the judge is saying. You catch only snippets of her carefully chosen words. Something about "spoliation of electronic evidence." Something about "shifting all costs of electronic discovery to your client."

Your mind races. What is metadata? Who the heck was Zubulake? Did the judge just say "sanctions"?

The courtroom falls silent. Pinning you with her gaze, the judge inquires, "Do you have any questions, counsel?"

Your client looks at you sideways. Your partner inches her chair away from yours. You rise to speak, mouth dry, trying to summon words of repentance.

You wish that, six months ago, you had learned about new standards for electronic discovery.

Discovery New ABA Civil Discovery Standards

BY DON BIVENS

Don Bivens
Don Bivens is a partner in the litigation law firm Meyer, Hendricks & Bivens, P.A., in Phoenix. He is a Past Chair of the Computer Litigation Committee of the ABA Litigation Section and a Past President of the State Bar of Arizona. He can be reached at dwbivens@mhb-law.com.

Relax. This courtroom fantasy will never happen to you, because you are already taking steps to prevent it. This article will give you the basics about new standards for electronic discovery published as Amendments to Civil the Discovery Standards of the Litigation Section of the American Bar Association.[1] The Civil Discovery Standards do not carry the force of law, but they do make studied and serious attempt to summarize the law as it has evolved to date on issues of electronic discovery.

Trust me on this. Whether you are a trial lawyer, a transactional lawyer or a judge, if you have not yet faced issues of electronic discovery, you will. And soon. You will not need to look for e-discovery issues. They will find you, for the simple reason that most people, consciously or not, routinely store business and personal information in electronic formats.

Do you use a computer for word processing? Do you send e-mails? Do you use the Internet? Do you have a cell phone or personal digital assistant? If so, then you need to know what is happening out there with electronic discovery.

My goal in this article is to provide some practical checklists, based on the ABA's August 2004 Amendments to the Civil Discovery Standards, that every lawyer (and judge) should consider when addressing issues of electronic discovery. If I do this right, I hope you will keep this article within reach for awhile as a resource and a catalyst for your own thinking.

Let's start with avoiding malpractice.

Informing the Client About Electronic Evidence

When does a duty arise for a lawyer to tell

the client about the need to retain electronic information?

When a lawyer learns that litigation is probable, he or she should inform the client about the duty to retain electronic information to avoid spoliation of evidence.

The duty to preserve information before litigation may be different from the duty to preserve and produce information after litigation has started. But whatever its scope, the duty to preserve electronic information becomes more pronounced as litigation become more likely. It's a sliding scale.

What kinds of electronic information does a client have a duty to preserve? Information within the client's custody or control, which may include items on our first checklist:

Checklist for Potential Types of Electronic Information

- E-mail, including attachments and metadata (Metadata refers to information about when an e-mails was created, to whom it was sent, when it was opened, responded to, who received blind copies, etc.)
- Word processing documents
- Spreadsheets
- Presentation documents
- Graphics/animations/images
- Audio/video/audiovisual recordings
- Voicemail

Where might these types of electronic information be stored? Most electronic information is stored in platforms, which might be in the possession of the client, or of a third party under the client's control (like an employee or outside vendor). A checklist for potential platforms might include:

Checklist for Potential Types of Electronic Databases

- Networks
- Computer systems (hardware and software), including systems no longer in use, sometimes called "legacy systems"
- Servers
- Archives
- Backup or disaster recovery systems
- Tapes, discs, drives, cartridges and other storage media
- Laptops, personal computers, personal digital assistants
- Mobile phones/paging devices
- Audio systems, including voicemail
- Internet data/Web logs/cookies

If you are like me, some of the items on these two checklists might not automatically come to mind when advising a client about the duty to preserve information for potential litigation. But today all lawyers should be aware of the duty to preserve all relevant sources of electronic information, when the occasion arises. These two checklists are a good place to begin the discussion with your client about duty to preserve evidence.

Let's assume for a minute that your client wants to file a lawsuit, and you want to make sure that the opposing party does not discard potentially relevant electronic information before you can prepare and serve an appropriate request for production. I would suggest sending a letter to the opposing side reminding them of the duty to preserve potentially relevant information, including electronic information.

Here again, these two checklists might be a good starting place for naming specific types of electronic information and platforms that you think should be preserved. Of course, you need to make sure that your own client plays by the same rules of preservation that you request of the other side. If not, any checklist in your letter could become a checklist for the court's imposition of sanctions against your client for spoliation of evidence for failure to preserve relevant information for trial.

Discoverable Electronic Information

The same two checklists you just reviewed also can serve as starting points for requesting electronic information during discovery, or for responding to such requests. The amended Civil Discovery Standards recommend that Rule 34 requests for production clearly state whether a party is seeking production of electronic information. In the absence of such clarity, a request for "documents" should ordinarily be construed as including a request for information contained or stored in electronic formats.

A requesting party should specify whether electronic information should be produced in hard copy, in electronic form or, in an appropriate case, in both forms. Sometimes it may be tempting to ask for a disk of the opposing party's documents. But if you only get a disk of imaged documents, will you be missing the opportunity to see whether certain documents, in their original form, were rubber-banded or clipped together, or whether certain pages were marked or set apart from others. That's something to think about.

A party requesting electronic information also should give some thought to the following items:

Checklist for Requesting Electronic Information

- Specifying the format in which you prefer to receive the electronic data (such as its native—original—format or a searchable format)
- Asking for the production of metadata associated with the responsive data (remember, metadata is information that shows when the responsive electronic information was created, edited, sent, received or opened, etc.)
- Requesting the software necessary to retrieve, read or interpret electronic information if such software or vendors who can provide it are not available
- Inquiring as to how the data are organized and where they are stored

If you are the responding party, the Civil Discovery Standards recommend that if you produce information in electronic form, then ordinarily you need not also produce hard copy to the extent that the information in both forms is identical or the differences between the two are not material.

Discovery Conferences and Pretrial Orders

In today's litigation environment, almost every case involves an initial discovery conference between the parties as the prelude to an initial pretrial management conference with the court. The Civil Discovery Standards recommend that certain topics be the subject of every initial discovery conference and pretrial conference, including:

Checklist for Electronic Discovery Pretrial Conference

- The subject matter of any proposed electronic discovery, and the relevant time period for which such discovery might be sought
- Identification or description of those persons currently or formerly affiliated with the prospective responding party who are knowledgeable about the information systems, technology and software necessary to access potentially responsive data
- The potentially responsive data that exist, including the platforms on which, and the places where, such data may be found
- Data retention policies applicable to potentially responsive data, and preservation of such data, specifically addressing (A) preservation of data generated after the filing of litigation; (B) data otherwise customarily subject to destruction in the ordinary course; and (C) metadata reflecting the creation, editing, transmittal, receipt or opening of responsive data
- Whether potentially responsive data exist in searchable form
- The use of key terms or other selection criteria to search potentially responsive data for discoverable information
- Whether the parties can agree on the names of unaffiliated information-technology consultants who would be capable of serving them jointly, either in privately retained or court-appointed capacity
- The initial production of tranches or subsets of potentially responsive data to allow the parties to evaluate the likely benefit of producing additional data, without prejudice to the requesting party's right to insist later on a more complete production
- The allocation of costs

To make matters a bit more complicated, you also should remember that electronic information subject to discovery in litigation can include information that the client has deleted, but which in fact can still be retrieved (called "residual data" in the *Zubulake* case, which has produced four leading decisions in the area of electronic discovery).[2]

It turns out that when most of us push the delete button on our computer, we do not actually delete anything. We simply send the putative "deleted" information to another location in our computers. (More specifically, the underlying data stay in the same location; only the "address of the data" is deleted.) Even when we send a document to the recycle bin, we don't necessarily delete anything from our computer's hard drive. We simply make the selected document eligible to be written over by a new document, should such a need ever arise within the computer.

Given the massive storage space available on today's computers—even on laptops—I wonder how many of us common users will ever successfully remove anything from our computers. More likely, we will simply move stuff around and get it out of our way. Just remember that electronic information that you or your client may regard as "deleted" may still be retrievable on your computer and subject to duties of preservation and discovery.

As a practical matter, a relatively small number of people in any lawsuit, on either side, really understand what kinds of electronic information and platforms may exist that contain potentially relevant information. It might be wise to take an early Rule 30(b)(6) deposition of the opposing party's designated representative who knows about the technology and software necessary to access potentially responsive data. Unless you are comfortable with the subject yourself, it could be worth consulting your own information-technology expert to help you ask the right questions.

While I am on the subject of information-technology consultants, let me also touch on issues of attorney–client privilege and work product. The amended Civil Discovery Standards suggest experts as efficient and effective solutions to problems of privilege.

Attorney–Client Privilege and Work Product

The amended Civil Discovery Standards suggest that, where appropriate, parties should consider stipulating to a court order to ameliorate concerns about attorney–client privilege and work product that naturally arise in the context of electronic discovery. The suggestions include:

Checklist for Dealing With Attorney–Client Privilege or Work Product Concerns

- Appointing a mutually agreed-upon, independent information-technology consultant as a special master, referee or other officer or agent of the court such that extraction and review of privileged or otherwise

protected electronic data will not effect a waiver of privilege or other protection attaching to the data

- Providing that production to other parties of attorney–client privileged or attorney work-product protected electronic data will not effect a waiver attaching to the data.
- Setting forth a procedure for the review of the potentially responsive data extracted, which might include:
  - An initial privilege review by the producing party, with production of the unprivileged and unprotected data to follow, accompanied by a privilege log.
  - An initial review by the requesting party followed by:
    - Production to the producing party of all data deemed relevant, followed by
    - A review by the producing party for privileged materials.

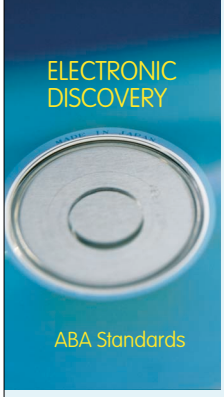
Obviously, any expert or opposing counsel who is permitted to launch a review of potentially privileged information will need to commit in writing to maintain any privilege subject to a final stipulation or order of the court. And, before agreeing to procedures that involve the review of potentially privileged documents by experts or by the opposing party, the lawyers on both sides will need to consider the potential impact such a review might have on the producing party's future ability to maintain any privilege in the face of future demands for the same electronic data by nonparties.

Having said all that, the Civil Discovery Standards generally recommend creative cooperation between the parties to solve what can be thorny issues of privilege and work product.

Which brings us to the final subject of who pays for all this electronic discovery anyway? The impecunious Plaintiff, the wrongly accused Defendant, or both?

Performing and Paying for Discovery

The amended Civil Discovery Standards identify a number of factors that the parties and the court should consider in resolving motions to compel or protect against the production of electronic information or



related software, or to allocate the costs of such discovery. Such factors include:

Checklist for Allocating the Costs of Electronic Discovery

- The burden and expense of the discovery, considering among other factors the total cost of production in absolute terms and as compared to the amount in controversy
- The need for the discovery, including the benefit to the requesting party and the availability of the information from other sources
- The complexity of the case and the importance of the issues
- The need to protect the attorney–client privilege or attorney work product, including the burden and expense of a privilege review by the producing party
- Whether the information or the software needed to access the information is proprietary or constitutes confidential business information
- Whether efforts have been made to confine initial production to tranches or subsets of potentially relevant data
- The extent to which production would disrupt the normal operations and processing routines of the responding party
- Whether the requesting party has offered to pay some or all of the discovery expenses
- The relative ability of each party to control costs and its incentive to do so
- Whether the responding party stores electronic information in a manner that is designed to make discovery impracticable or needlessly costly
- Whether the responding party has deleted, discarded or erased electronic information after the responding party knew that litigation was probable and, if so, the responding party's state of mind in doing so

Conclusion

The checklists and commentary in this article are my best effort to share the main points of the amended Civil Discovery

Standards from the ABA Litigation Section, but my shorthand observations are no substitute for a close reading of the amended standards in their full glory. I recommend that you take a minute right now to download the guidelines for free from the Web site of the ABA Litigation Section, www.abanet.org/litigation/home.html. While you are there, I also recommend that you become a member of the Litigation Section. There is a wealth of information available online to Section members.

At a minimum I hope these checklists serve to stimulate your own further thinking on the topic of electronic discovery. If you have any questions, suggestions or comments on this subject, I would be happy to hear from you. I suspect that all lawyers and judges, unless we are very careful, are likely to be learning new things about electronic discovery, good and bad, in the daily course of our practice. If you come across something that works well for you and your client in this emerging area, pass it on. That's what being a member of the profession is all about.

endnotes

1. The August 2004 Amendments to the Civil Discovery Standards can be accessed online at the ABA Litigation Section Web site: www.abanet.org/litigation/taskforces/electronic/
2. *Zubulake v. UBS Warburg LLC,* 217 F.R.D. 309, 313 n.19 (S.D.N.Y. 2003):
   "The term 'deleted' is sticky in the context of electronic data. Deleting a file does not actually erase that data from the computer's storage devices. Rather, it simply finds the data's entry in the disk directory and changes it to a 'not used' status—thus permitting the computer to write over the 'deleted' data. Until the computer writes over the 'deleted' data, however, it may be recovered by searching the disk itself rather than the disk's directory. Accordingly, many files are recoverable long after they have been deleted—even if neither the computer user nor the computer itself is aware of its existence. Such data is referred to as 'residual data.'" (internal quotations and citations omitted)