

# YOUR METADATA'S SHOWING: DO YOU KNOW WHAT OPPOSING COUNSEL SEES?

L. Allison McKeel

---

*The proliferation of computers, PDA's, cell phones and other devices has created a wealth of hidden information that lawyers in any type of practice can no longer afford to ignore. "Metadata" (information about a document that does not appear on paper when a document is printed) and other electronic information that remains on a computer even after documents are deleted, have created a whole new array of ethical and legal issues facing lawyers. The issues arise in everyday practice and in litigation-in small and large cases.*

*In order to meet the minimum standards for competent and zealous representation, attorneys in any area of practice, from criminal law to intellectual property, must be aware of available electronic information and the issues related to use, preservation, and production of such information.*

## THE DANGERS OF BEING AN OSTRICH—METADATA

Every attorney should have at least basic knowledge of metadata and its related issues in order to avoid questions of improper disclosure of information adverse to a client. One issue is the transmission of documents by e-mail or in other electronic format such as on a CD or diskette, which contain metadata. Attorneys often send routine correspondence or documents as e-mail or an attachment to e-mail. The electronic version of these documents as opposed to the paper version—contains a variety of hidden data, or "metadata." Metadata can be revealed in a several ways<sup>[1]</sup>, and includes: the date of creation of the document, the file path on your computer, the original and subsequent authors, the date and number of any revisions, and in some cases the changes made in various versions of the document. This information occurs in varying forms in Word, WordPerfect and Adobe documents.

The file path alone can raise confidentiality issues, when, for instance, you save a document under a file name such as C:\My Documents\ Client Name\Current Litigation Files \Jones Matter\Letter to Opposing Counsel. Upon viewing this information, the other party is alerted that your client may have other current litigation pending. The party may conduct further investigation and discover prejudicial information that might not otherwise have been revealed.

Additionally, if you use one document as a template, make revisions, and then save it under another name, the original creator (author) is still displayed in the document properties. Consequently, if you receive discovery requests, a brief, or other document from opposing counsel on a disc or by e-mail, modify the document, and save it, the document properties (metadata) will still show the first firm as the creator of the document. This could be embarrassing and a strategic disadvantage for your client, particularly if the firm that created the document is now the firm to whom you are sending a later version.

These are limited examples of the problems—and potential ethical issues that can arise from the lack of awareness of metadata.<sup>[2]</sup> Unless you are familiar with the details of metadata, and unless you take consistent and effective measures to protect against adverse use of such information, you are better off sending communications by traditional mail and fax methods.

## THE PERILS OF BEING A DINOSAUR—ELECTRONIC DATA IN LITIGATION

The wealth of electronic information contained on computers and other electronic devices mandates a need to have a basic understanding of electronic data and its place in litigation. Several recent federal cases highlight the perils of ignoring increasingly accepted principles regarding electronic evidence and discovery in litigation.

In *Zubulake v. USB Warburg*, 94 Fair Empl.Prac.Cas. (BNA) 1, 2004 WL 1620866 (S.D.N.Y.), the court issued monetary sanctions and allowed an adverse inference jury instruction against the employer in an employment discrimination case for destruction of electronic evidence. This was despite the fact that counsel for the employer had issued instructions to the client's employees at the outset of litigation to retain relevant electronic information. The court found that although counsel had initially notified company personnel of their duty to preserve evidence, counsel had subsequently failed to properly monitor compliance with their preservation instructions. The court emphasized that counsel's duty to locate relevant evidence requires counsel to "become fully familiar with her client's document retention policies, as well as the client's data retention architecture," and

that “[c]ounsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched.”[3]

In *Wiginton v. CB Richard Ellis*, 2003 WL 22439865 (N.D.Ill.), the court held that the defendant employer in a sexual harassment case had acted in bad faith for failure to change its normal document retention policy after litigation ensued. Defendant destroyed backup tapes of the company’s e-mail system and failed to preserve the hard drives of relevant employees, including Plaintiff’s former supervisor, after Plaintiff served notice on Defendant to preserve electronic data. The Court noted that the “question of intent and/or bad faith. . .may encompass not only direct destruction, but also ‘willful blindness.’”[4] The court allowed the Plaintiff to conduct additional discovery to prove the extent of damage from such destruction.

Given increasingly accepted standards for the preservation, discovery and production of electronic evidence, it is incumbent upon attorneys to have basic familiarity with computer systems and data, or to enlist the assistance of experts, in order effectively advise clients in all types of cases.

## **BASIC STEPS FOR HANDLING ELECTRONIC-DATA IN LITIGATION**

Although there appear to be no cases in Missouri or in the Eighth Circuit addressing electronic evidence or discovery issues, there is substantial authority in the Seventh Circuit, the Illinois federal district courts, and other jurisdictions, that has established recognized procedures for preserving, discovering, and producing electronic evidence in litigation. The following steps should be implemented before and after litigation to best protect your clients and to assure compliance with the applicable rules and caselaw:

1. **Have A Document Retention (Destruction) Policy in Place.** Before any issue of litigation arises, having a proper document retention policy in place and properly enforced can significantly limit a client’s exposure related to destruction of documents prior to notice of any legal claim or action.[5] A document retention policy dictates which documents are routinely kept, which are routinely destroyed, and the procedure and timing for the destruction of documents.
2. **Issue a Proper “Litigation Hold” on the Destruction of Evidence.** Counsel must advise clients of the duty to preserve electronic evidence relevant to an action, once the client is reasonably on notice of a pending claim or action.[6] The duty to preserve may attach before a lawsuit is filed. It is essential to communicate fully with the client at the outset of representation to determine all people with relevant information who must be notified of the litigation hold, and to determine the scope of information that is potentially relevant and must be included in the litigation hold.
3. **Send a Preservation Letter to the Opposing Party and Necessary Third Parties.** As early as possible in the litigation (in some cases it is appropriate before a claim or action is filed), a letter should be sent to the opposing party and any necessary third parties, advising that certain electronically stored information is at issue in the case or may be relevant evidence in the case, and requesting the party to preserve any such evidence. Sending a preservation letter puts the other parties on notice to stop their normal document retention (destruction) policies, and can trigger sanctions by the Court against a party to the litigation, if relevant documents are destroyed after such notice. Sample preservation letters to opposing parties and to third parties are available at <http://www.discoveryresources.com> and <http://www.krollontrack.com>.
4. **Preserve a Forensically Sound Copy of Any Relevant Computer Hard Drives in the Client’s Possession.** This is essential to preserving the integrity and admissibility of valuable evidence that is often in your own client’s hands. It also permits the client to continue operating its computer equipment in the normal course of business, while preserving evidence which is potentially crucial to the client in a lawsuit. The data can be analyzed at a later date if litigation becomes a reality. It further protects against later claims of spoliation by the opposing party, if a lawsuit is filed. In order to preserve the forensic value of a hard drive, it is critical to obtain a copy before the hard drive is otherwise examined or analyzed (i.e. by employees of the client), because even turning on and off the computer alters data contained on the computer.

Preservation can be accomplished in two relatively inexpensive ways. First, the hard drive can be removed from the computer and replaced with a new hard drive approximate cost: \$100-150 depending on the replacement hard drive and a relatively simple procedure). Second, a mirror image of the hard drive can be made (approximate cost \$400-700 and should be done by a computer forensic expert). In either case, the chain of custody and other evidentiary procedures must be observed and documented. Ideally,

either procedure should be conducted by an outside expert to assure the forensic integrity of the data and admissibility at trial.[7]

[ In the event of litigation:]

5. Have a forensic analysis conducted of the computers in your clients' possession. The cost of such analysis is not always as prohibitive as imagined. For example, a very basic search to determine if any computer "wiping" or "cleansing" software was installed and used to delete information on the computer could be done quickly and inexpensively. A more thorough search for existing and deleted information on a single computer can be done in the range of \$3,000-\$10,000, depending on the extent of information searched for. The cost benefit of such a search can be exceptional, if the search uncovers a "smoking gun" document which results in early termination of the litigation. This can be the case in non-competition, trade secrets, and employment cases, among others. While cost may be a prohibitive factor in any particular case, the client should have the opportunity to make an informed choice regarding such expenditures.
6. Draft Discovery Addressing Electronic Evidence Issues. Although the Federal Rules of Civil Procedure and parallel state rules include the duty to produce electronic data under the standard discovery provisions[8], discovery requests in any case seeking electronic data (including the electronic version of e-mail) should be tailored specifically to identify and request relevant electronic data based on the facts of your case.[9] Sample discovery requests are available at <http://www.krollontrack.com> and [www.discoveryresources.com](http://www.discoveryresources.com).[10]
7. Complete Discovery of Other Parties' Electronic Data. The producing party ordinarily bears the cost of production of electronic data. In order to limit the cost of electronic discovery, the parties may confer and agree to limit the scope of discovery at the outset of litigation. If the parties have comparable resources, negotiation can often effectively limit electronic discovery to the most relevant information. If either party is unduly burdened by a request for production, it may make a motion for cost-shifting. The Court may shift the costs of discovery based on several factors.[11] The more knowledge counsel has about the electronic data at issue, the more effectively he or she can direct and control the costs of electronic discovery.

---

## FOOTNOTES

[1] For example, in Word documents, click on the File menu, then Properties or Versions. Alternatively, click on the Tools menu, then Options, then the Security tab, and deselect "Remove personal information from file properties on save." Then still under Options, the Print tab, and select Include with Printing, "Document Properties." Then print the document.

[2] For more comprehensive articles describing the information available in metadata and ways to eliminate such information from your documents, see Fedder, "The Ethics of "Hidden" Information in Electronic Documents," St. Louis Lawyer, April 2004 (discussing the duty under the Missouri Rules of Professional Conduct to protect against disclosure of information related to a representation of a client); and Hricik, "The Transmission and Receipt of Invisible Confidential Information." [www.Hricik.com](http://www.Hricik.com), 2003 (detailing the information readily available as metadata and methods of removing such information-cautioning that no method is completely effective).

[3] 2004 WL 1620866, at \*8.

[4] Quoting, *Danis v. USN Communications, Inc.*, 53 Fed.R.Serv.3d 828, 2000 WL 1694325 at \*32 (N.D.Ill.).

[5] Such a policy will not protect against sanctions for destruction of relevant evidence after notice of a claim or action. See, e.g., *Rambus, Inc. v. Infineon Techs. AG*, 2004 WL 383590 (E.D.Va.) (defendant allowed to introduce evidence of Plaintiff's document destruction practices where Plaintiff instituted a "Shred Day" after notice of Defendant's lawsuit, and Plaintiff did not deny that it destroyed some documents because of their discoverability.)

[6] *Wiginton v. CB Richard Ellis*, 2003 WL 22439865, at \*4.

[7] Two companies that perform mirror hard drive imaging as well as a full range of electronic discovery services are Fios ([www.fiosinc.com](http://www.fiosinc.com)) and Kroll Ontrack ([www.krollontrack.com](http://www.krollontrack.com)). Both companies' websites have informative

articles and newsletters, and free online CLE programs regarding electronic evidence and discovery. Fios also provides a free, comprehensive and very readable guide, "A Process of Illumination: The Practical Guide to Electronic Discovery," which can be downloaded or ordered in print.

[8] *In re Verisign, Inc. Securities Regulation*, 2004 WL 2445243 (N.D.Cal.); *In re Plastics Additives Antitrust Litigation*, 2004 WL 2743591 (E.D.Pa.).

[9] For cases involving misappropriation of computer data, counsel should consider a claim under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C.A. 1030. For an excellent article on claims under the CFAA, see Lenard, "Using the Computer Fraud and Abuse Act to Combat Improper Employee Competition," *St. Louis Lawyer*, April 2004, p. 16.

[10] These discovery requests are comprehensive and may be simplified where the computer data sought is limited.

[11] See, *Byers v. Illinois State Police*, 53 Fed.R.Serv. 740, 2002 WEL 1264004 (N.D.Ill), at \*10-12; *Rowe Entertainment, Inc. v. The William Morris Agency, Inc.*, 2002 WL 63190, at \*6 (S.D.N.Y.); *Zubulake v. USB Warburg*, 219 F.R.D. 209 (S.D.N.Y. 2003).

*Allison McKeel is Senior Counsel with Bobroff, Hesse, Lindmark & Martone, PC, where she practices Employment, Construction, and Commercial Litigation. She is a member of the Steering Committee of BAMSL's Federal Litigation and Practice Committee. The author would like to thank Richard Perkins and Mindy Mahn of Bobroff, Hesse for their assistance in preparing this article. For more information contact: allisonmckeel@bobroffhesse.com or (314) 862-4681.*

---