

Metadata, ESI, and the Federal Discovery Rules

BY LAZAR EMANUEL

[Research and guidance for this Article were contributed by my son David, IT consultant.]

In last month's NYPRR, I offered a definition of the term "metadata" and cited a number of examples illustrating how metadata can lead to the inadvertent disclosure of privileged matter and of client confidence and secrets. I reserved the following question, among others, for expanded discussion in this issue:

What is the impact of amended Federal Rule 26 on these issues [i.e., the issues raised by metadata as one potential element in the discovery process]?

All data created and accessible electronically, including meta-data, is referred to in the new federal discovery rules as electronically stored information or ESI. (It is sometimes also referred to by others as e-data.)

The new federal discovery rules became effective on December 1, 2006. The major provisions are embodied in FRCP 16, FRCP 26, FRCP 33, FRCP 34, FRCP 37, and FRCP 45. In general terms, the new rules are designed to:

- recognize the increasing significance of ESI to the discovery process
- reflect the difference between ESI and other forms of discoverable data
- emphasize the obligation to maintain ESI as a potential source of evidence in discovery
- affirm the responsibility to protect privileged and protected information from disclosure
- create machinery for expeditious pretrial cooperation among litigants in the discovery process
- provide for the preservation by the parties to litigation of all potentially discoverable evidence
- consider and determine the cost of producing ESI if a party argues that the ESI is not readily accessible
- limit sanctions for non-production of ESI when the ESI has been lost as the result of the routine operation of an electronic information system, so long as the operation is conducted in good faith.

California Judge Awards Discovery of Data in RAM

Since my article in June, a federal magistrate in California has decided that, under the new federal discovery rules, the plaintiff in a copyright infringement action may compel discovery of ESI housed temporarily on a computer as RAM (random-access memory). *Columbia Pictures Industries, et al. v. Bunneli, USDC CDCA, Case No. CV 06-1093 FMC(JCx) (2007)*. [Note: RAM is an initial and transitional computer storage area which houses electronic data as it is being created on the computer for a period of about six hours. It has been described as a bucket with a small hole at the bottom which gradually allows data routed to the bucket to seep into the computer's hard drive.]

How does a decision providing access to data in RAM affect access to metadata? Very simply - because both RAM and metadata are technological operating processes built into the mechanism which drives computers and which are essentially uncontrolled and uncontrollable by the user. Both are created inadvertently as the user works on a document; both are accessible or can be made accessible in the discovery process; and both are potential sources of evidence relevant to litigation or a threatened litigation.

The Report of the Judicial Conference Committee which led to adoption of the new electronic discovery rules clearly anticipated that metadata would be included in the definition of ESI.

During the study of electronic discovery, the Committee learned that reviewing electronically stored information for privilege and work product protection adds to the expense and delay, and risk of waiver, because of the added volume, the dynamic nature of the information, and the complexities of locating potentially privileged information. Metadata and embedded data are examples of such complexities; they may contain privileged communication, yet are not visible when the information is displayed on a computer monitor in ordinary use or printed on paper.

Of course, until the courts begin to decide cases requiring application of the new discovery rules to particular instances of allegedly privileged or protected metadata, we will not know all the answers. However, the court's decision in *Columbia Pictures* would appear to make metadata as vulnerable to discovery as information stored in RAM.

Facts in *Columbia Pictures*

In *Columbia Pictures*, the defendants maintained a website under the name Torrent Spy. The purpose of the business was to assemble and distribute to users electronic data which would enable the user's computer to access and assemble a full-length film. Customers requested the data electronically from the defendants' server. In the process, the server was able to create a log file which could record and maintain the customer's IP address in RAM. However, the server's logging function was optional and could be disabled by the defendants. Defendants chose to disable the function on the server, but although the data never seeped to the hard drive (server), it was nevertheless retained temporarily in defendants' RAM.

At some point close to the initiation of discovery by plaintiffs, defendants contracted with a third party, Panther, to maintain incoming user data on its servers. As a result, the data was no longer channeled through defendants' RAM. Because Panther did not maintain logs on its servers, the data was retained temporarily only in Panther's RAM and was then lost.

Columbia Pictures served a preservation motion on the defendants. The court decided, in effect, that the defendants were in control of the data, that the data in Panther's RAM belonged to defendants, and that defendants were under an obligation to preserve the data in Panther's RAM for discovery by Columbia. The court rejected defendants' argument that they would be unduly burdened by the cost and effort required to preserve and produce the data in Panther's RAM. However, the court did not impose sanctions on the defendants. It found that

...defendants' failure to retain the server log in RAM was based on a good faith belief that preservation of data temporarily installed only in RAM was not legally required. Consequently,

the court finds that evidentiary sanctions against defendants for spoliation of evidence are not appropriate.

Unfortunately, the court's opinion offers no insight or guidance on the technology required to preserve data stored in RAM. It does, however, limit its impact to the facts of the case:

The court emphasizes that its ruling should not be read to require litigants in all cases to preserve and produce...information that is temporarily stored in RAM. The court's decision ...is based in significant part on the nature of this case, the key and potentially dispositive nature of the Server Log Data which would otherwise be unavailable, and defendants' failure to provide what this court views as credible evidence of undue burden and cost.

Application to Metadata

Because metadata, like RAM, is created inadvertently and is so difficult to find and isolate, many of the same issues which were faced by the judge in *Columbia Pictures* will confront judges who have to decide motions to preserve and produce metadata. Unless the destruction of metadata has been conducted willfully or in bad faith, the principal issue for the court will be the cost to the producing party of preserving the data or of putting in place a procedure for separating privileged and protected data from data which may have evidentiary value in litigation. If the good faith of the disclosing party in withholding or destroying data is put in issue, the court will have to inquire into the facts to determine if sanctions are appropriate.

Whether applied to data in RAM, or to metadata, or any other ESI, the courts' obligation to inquire into a party's reasons for withholding data in discovery is circumscribed by two features of the new federal rules:

1. A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. FRCP 26(b)(2)(B); and
2. The courts may not impose sanctions on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system. FRCP 37(f).

Both of these exceptions to the general rule requiring production of evidentiary ESI raise several fundamental questions:

- a. Do federal judges have enough training and knowledge in information technology and the Internet to resolve the technical questions they will confront in interpreting the rules?
- b. If, as it is reasonable for us to assume, the judges do not have sufficient knowledge, how are they to acquire it in a fact-specific situation without slowing the proceedings up unreasonably?
- c. If, in a discovery proceeding, a party argues that providing access to ESI will impose an undue burden and excessive cost, how will the court decide among alternative technologies for making

the information available; how will it determine the cost to the party; and by what standards will it measure whether the technology is burdensome or the cost excessive?

- d. If a party argues that the information sought by the other party has been lost in the good-faith operation of its electronic system, what technology will the court need to know to understand the party's operating system and whether the system can help it to determine whether the loss of evidence was inevitable, accidental, inadvertent or deliberate?

My personal view is that these are overwhelming burdens for the courts, and that over time and in the light of decisions yet to come, many of the new rules will require clarification and amendment. The battle between law and technology has just begun.

Two Other Issues

In my June article on metadata, I raised two other issues:

1. Does a lawyer who sends a document electronically have an obligation to exercise reasonable care to ensure that the document does not inadvertently disclose a secret or confidence of her client through metadata? If so, what constitutes "reasonable care"?
2. Does a lawyer who receives an electronic document from opposing counsel have an obligation: (a) to refrain from researching, reviewing and using metadata embedded in the document; and/or (b) to notify the sender that he knows or suspects that the document contains metadata which she appears to have forwarded inadvertently?

In this article, I will tackle only Issue 1. I will reserve Issue 2 for another article. I will discuss Issue 1 from the perspective of the lawyer who controls and maintains the ESI.

A lawyer in this position has two potentially conflicting duties with respect to ESI that becomes or may become the subject of threatened or pending litigation:

- a) to preserve information he knows, or reasonably should know: (i) that is or may be relevant to the litigation; (ii) that will or may lead to the discovery of admissible evidence; or (iii) that may be, or has been, requested during discovery; and
- b) to prevent the disclosure of information which is privileged or which may disclose a client's confidences or secrets.

The duty to protect the client's confidence and secrets when transmitting or disclosing ESI is unchallenged by anyone. It is recognized in the Ethics Opinions of the ABA and of the states. As it relates specifically to metadata as an element of ESI, the duty has been confirmed by the NYSBA in two separate opinions:

The protection of the confidences and secrets of a client are among the most significant obligations imposed upon a lawyer. As explained in EC 4-1, "...The observance of the ethical obligation of a lawyer to hold inviolate the confidences and secrets of a client...facilitates the full

development of facts essential to proper representation of the client..." *Opinion 749, December 14, 2001.*

The Lawyer's Code of Professional Responsibility prohibits lawyers from "knowingly" revealing a client confidence or secret....When a lawyer sends a document by e-mail...a lawyer must exercise reasonable care to ensure that he or she does not inadvertently disclose his or her client's confidential information. *Opinion 782, April 15, 2004.*

Because metadata is generally created inadvertently as part of the process by which an electronic document is fixed or finished, and also because it is difficult for the ordinary computer user to identify and remove metadata, the ABA has endorsed and promoted various methods "to limit the likelihood of transmitting metadata in electronic documents." *Formal Opinion 06-442, August 5, 2006.* Included in these methods are:

- Avoid creating some metadata in the first place - forego the use of redlining and the insertion of comments.
- Delete comments when the article is finished.
- Use a program designed to "scrub" metadata before sending an electronic document to others.
- Study and utilize new methods and programs in articles and technical manuals, and on the Web, to control metadata.
- Transmit vital documents in hard copy, or by fax, or after conversion to PDF.
- As a last resort, negotiate a confidentiality agreement, or apply for a protective order, to "pull back" or prevent the introduction as evidence of, the metadata the lawyer wishes not to divulge.

The ABA Opinion was released a few weeks after the Supreme Court approved the new discovery rules. The Opinion noted that the rules contain provisions allowing a producing party to "pull back" privileged information and work product under certain circumstances. But the Opinion omitted any discussion of the impact of the new discovery process on metadata.

Of course, metadata (like all other ESI) must not be made inaccessible if it constitutes evidence in a threatened or pending litigation and if it is neither privileged nor protected as a client confidence or secret. As the Judicial Conference Committee stated in its Report, "A party that makes information 'inaccessible' because it is likely to be discoverable in litigation is subject to sanctions now and would still be subject to sanctions under the proposed amendment."

Let's consider again the example I used in the June article of the senior partner in law firm A who bills his client at his own hourly rate for the drafting of an involved contract when all the work was done by an associate. Metadata will probably reveal that the associate created the contract on his own computer. Suspecting that he has been taken, the client retains new firm B to recover the difference in fees and for other remedies. New firm B seeks discovery of the electronic data showing the name of the lawyer who drafted the contract. If the data has been scrubbed or obliterated, law firm A and the senior partner may be guilty of spoliation and subject to evidentiary sanctions.

In its copyright infringement action, *supra*, Columbia Pictures asked the court to impose evidentiary sanctions against the defendants on account of their alleged "willful failure to preserve, and intentional

spoliation of, the Server Log Data." In denying the motion, the court said:

... absent exceptional circumstances, a court may not impose sanctions under the discovery rules based on a party's failure to provide electronically stored information lost as a result of the routine, good faith operation of an electronic information system. F.R. Civ. 37(a). A "good faith" operation may require a party to modify or suspend certain features of ...operation to prevent the loss of information, if that information is subject to a preservation obligation."

Under this standard - and in the case of the partner in law firm A - the installation of a program which identifies and removes all metadata indiscriminately- i.e., a program that "scrubs" metadata electronically - would not pass muster. Because its Formal Opinion 06-442 was issued before the new federal discovery rules became effective, the ABA's recommendation of scrubbing ESI to remove metadata must be construed as inadvertent but misguided.

As we saw in my June article, many tools for "scrubbing" metadata and other ESI are now on the market. These and other tools designed to control ESI must now be reexamined under the new federal rules. Law firms need to put in place programs that combine good-faith supervision by their lawyers and IT specialists with the technology to identify and preserve evidentiary data without jeopardizing either privileged data or data containing client confidences and secrets.

Lazar Emanuel is the publisher of NYPRR.