Center *for* Professional Responsibility

What Lurks Within: Hidden Metadata in Electronic Documents Can Win or Lose Your Case

By Eileen B. Libby

April, 2007

Every lawyer, as well as every lawyer's employee, should be aware of the potential liability that may be found in metadata. The easiest way to define "metadata" is to say that it is "data about data." Metadata can provide both essential and non-essential information, as well as contextual information. Web browsers automatically download stored metadata to make files easier and quicker to access. One of the most popular—and useful-- forms of metadata is the audio digital file "tag," additional information displayed upon playback of an MP3 file on a computer or portable device such as an iPod.

Metadata takes several forms. File system metadata created by programs such as Word and Excel can include the following: file name, original author, information regarding by whom and when revisions were made, number of pages, number of characters, file size, date created, date modified, and date printed. Recipients of Word documents can view the document's metadata by clicking on "File" and selecting "Properties." E-mail metadata can provide additional information, including the sender's domain, the route a message has traveled over the Internet, and where delays may have occurred between sending and receipt.

The metadata in spreadsheets can be mined to find out the formulas behind the calculations. In *Williams v. Sprint/United Management Company*, 230 F.R.D. 640, 652 (D. Kan. 2005), terminated employees brought a class action and sought Excel spreadsheets with all metadata intact, including embedded formulae. The court held that under "emerging standards of electronic discovery" metadata ordinarily visible to users of Excel spreadsheets "should presumptively be treated as part of the 'document' and should thus be discoverable."

One also may be able to uncover previously deleted text if the embedded data is still present in the "bowels" of the file. An opposing party or even a judge, can turn Word's "Track Changes" on, thus revealing the revisions in a deactivated document, including privileged or protected information such as inserted editorial comments or settlement proposal strategies. Portable Document Format (PDF) documents also may contain potentially harmful metadata, although less than in other types of documents,

Application and file system metadata derived from electronic documents and files has the potential to be win-or-lose evidence. In one of the product liability lawsuits regarding the prescription drug Vioxx, metadata revealed that the manufacturer, Merck, edited out negative information from a drug study.

One federal jurist stated in an opinion that the risk of waiver is "one of the most challenging aspects of discovery of electronically stored information."

Consequently, metadata is becoming an increasingly important part of electronic discovery. Recent changes to the Federal Rules of Civil Procedure make metadata routinely discoverable as part of civil litigation. Parties to litigation are required to maintain and produce metadata as part of discovery, and spoliation of metadata can lead to sanctions. They may negotiate to exclude metadata from produced documents in the obligatory meet and confer under the new rules, but without an agreement to that effect, the parties must produce the metadata.

But what if a lawyer is on the receiving end? Is there an obligation to refrain from viewing the metadata or reviewing it to get a glimpse of an opponent's legal strategy? Is it unethical to use sleuthing techniques to mine the other side's hidden data? Answers may be found in ABA Standing Committee on Ethics and Professional Responsibility Formal Ethics Opinion, 06-440, which interprets Model Rule 4.4 (Respect for Rights of Third Persons). The Rule was revised in 2002 as part of the Ethics 2000 amendments.

Rule 4.4(b) requires a lawyer who receives materials sent inadvertently only to notify the lawyer who sent them. The receiving lawyer is not prohibited from reviewing the materials, nor is the lawyer required to abide by the sending lawyer's instruction as to disposition of the materials. In its opinion, the ABA Ethics Committee states that the rule "requires only that a lawyer who receives a document relating to the representation of the lawyer's client and who knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender. The Rule does not require refraining from reviewing the materials or abiding by instructions of the sender."

The Ethics Committee recommended that lawyers take steps to guard against the disclosure of metadata, including "scrubbing" metadata from documents prior to production and entering into "clawback" or nonwaiver, agreements, under which inadvertently produced material is returned without waiver. Recent amendments to the Federal Rules of Civil Procedure and recently proposed amendments to the Federal Rules of Evidence both recommend such agreements.

Several states have issued opinions regarding metadata and have reached different conclusions. Maryland Bar Association Committee on Ethics Opinion, 2007-09, "Ethics of Viewing or Using Metadata," follows an approach similar to that taken in the ABA opinion. Because Maryland has not adopted Model Rule 4.4(b), its lawyers are not under an obligation to notify an adversary of an inadvertent production. In addition, the Maryland opinion concludes that a lawyer has an ethical obligation to take "reasonable measures to avoid the disclosure of confidential or work product materials" contained in metadata. In contrast, Florida Bar Opinion 06-2 states that a lawyer has both a duty to refrain from reviewing or using metadata and a duty to notify an adversary of inadvertent production.

The New York Committee on Professional Ethics has examined the metadata problem in several opinions. In Opinion 749, the New York Committee took the view that using available technology to view metadata violates New York ethics rules that prohibit conduct "involving dishonesty or fraud" and conduct "prejudicial to the administration of justice." Thus, New York lawyers are prohibited from making "use of computer software applications to surreptitiously 'get behind' visible documents or to trace e-mail."

In Opinion 740, which addresses the question of inadvertent disclosure, the New York Committee held that a lawyer who receives confidential materials when it is clear that the materials were not intended for the receiving lawyer should not examine the materials once the inadvertence is discovered and should notify the sender. The recipient should abide by the sender's instructions as to the need to return or destroy the materials.

Is there an ethical obligation to guard against the inadvertent disclosure of client confidences and secrets contained in metadata? Although in Opinion 782, the New York Committee did not directly state that a lawyer who transmits documents containing metadata reflecting client confidences or secrets violates ethics rules, it concluded that a lawyer should "use reasonable care when transmitting documents by email to prevent disclosure of metadata containing client confidences or secrets." The New York Committee reminded lawyers that this duty "may, in some circumstances, call for the lawyer to stay abreast of technological advances and the potential risks in transmission," but rejected the view that a lawyer has an affirmative duty to remove metadata whenever documents are sent to opposing counsel or publicly disclosed.

How can a lawyer guard against disclosing information contained in metadata? There are many ways to clean or "scrub" documents of embedded hidden data, for example, programs such as iScrub, 3B Clean, PCG's Metadata Assistant, and Workshare's Professional 4's "Hidden Data." Later versions of Adobe Acrobat contain many new tools to help lawyers avoid an inadvertent disclosure. Sending documents in Macromedia Flash format also is an option. Microsoft itself has the "Remove Hidden Data" tool that permanently removes hidden and collaboration data such as change tracking and comments from documents edited with MS Word, MS Excel, and MS PowerPoint. Another solution is to use WordPad, a stripped-down word processor in Windows, or save the file in Rich Text Format (RTF).

However, if a document is subject to discovery, scrubbing should not be done to the original file because it can alter it permanently. Given the amendments to the Federal Rules of Civil Procedure, it is inadvisable to scrub metadata without first reaching an agreement on the contours of electronic production with one's opponent. Amended Rule of Civil Procedure 34(b) permits a requesting party to specify the format in which it would like to have the electronically stored information produced. The expectation is that most will request that the data be in "native" format in order to preserve metadata, meaning that the electronic information must be produced as it is maintained and used.

The wise lawyer will establish an office or firm-wide policy that can help ensure security over documents, thus protecting their integrity and security before the "Send" button ever is pressed. The only way to eliminate all risks, however, is to stick to old-fashioned hard copies of documents.

Eileen B. Libby is Associate Ethics Counsel to the American Bar Association's Standing Committee on Ethics and Professional Responsibility.