

UNDERSTANDING METADATA

One of the principal ways electronic documents differ from paper is the existence of metadata. With a printed document, what you see is what you get, whereas with an electronic file, what you see on the computer screen is only just the beginning. What is not visible typically with an electronic document is the corresponding digital metadata that complements every electronic file.

Due to its nature, however, metadata can create significant hazards for lawyers, especially those who are unaware of its existence or import. In their use of the tools of modern technology – desktop and laptop computers, personal digital assistants, e-mail, and all of the software that makes them useful – lawyers everyday encounter hidden, digital metadata whether they know it or not. Whether routinely creating their own digital documents and data, or handling electronic records as evidence, lawyers constantly create, shape and disturb metadata and, as a result, are exposed to a variety of potential risks. Developing an understanding of metadata is therefore essential for every attorney in practice today, regardless of their technological know-how or resources.

Defining Metadata

So, what is metadata exactly? Metadata is vital information hidden within an electronic file about the file data. By accessing an electronic file's metadata, a user can access a wealth of background and other demographic information about the file. Some examples of metadata include the file's name, location, format, size and type, as well as information describing how, when, and by whom the file was created, accessed, and modified and the dates and times of each, to list just some of the data potentially present. Metadata is thus hidden background data about the data itself.

There are primarily two kinds of metadata. Data that is embedded and hidden within the file itself is called *application metadata*. Such information follows each file wherever it goes. In contrast, *system metadata* is stored externally and used by the computer's operating system to keep track of each file. By design, computer software applications compile and use metadata to quickly perform countless tasks. So, in large part, metadata is what makes technology so useful – allowing us to quickly sort through mountains of virtual data, locate specific information, and revise, restore or duplicate assorted versions of electronic records.

While some metadata requires expert forensic investigation to uncover, other more basic types can be accessed with a simple click of a mouse. For example, by selecting "File/Properties" from the drop-down menu in the most commonly-used office software applications, a user can easily identify the dates and times when a document was created, last accessed and last modified, as well as the total editing time. All in all, there are potentially hundreds of distinct fields of metadata, each field supplying unique information about a given file. In fact, the most commonly used office software applications hold over 80 different metadata fields within each file. And this does not include the popular collaboration tools now available that enable multiple users to insert and

exchange editorial data in these files, automatically adding more metadata with each user and keystroke.

The Dangers of Metadata for Lawyers

Metadata has been referred to as the fingerprints of an electronic file as it is created, modified, and even deleted over time. When a digital file is erased, forensic evidence of the file is left behind in the system metadata. So, while lawyers and their staff are tapping away at their keyboards and personal digital assistants, the software applications they are using are compiling a digital transcript of everything they are doing. But, because metadata is not visible unless specifically accessed, most users are unaware it is there.

One of the most important things to understand about metadata is that it is ubiquitous – embedded automatically within every single electronic record. A digitally recorded message left on voicemail holds metadata about the date, time and origin of the call. The same is true of a fax transmission. Metadata is especially abundant in electronic mail, carrying data about the message's origin and destination, transmission time and path, and other complex routing information.

Although metadata can be quite technical, all metadata is information and thus can be relevant to a lawyer's practice or a client's matter. Because it is information, metadata is evidence and, therefore, is potentially discoverable just like other kinds of electronic data. While most of the time metadata may have limited value or relevance, it will be discoverable if it provides information that is material to issues that are in dispute or useful to establish a foundation for other underlying electronic evidence. Therefore, it is important for lawyers to know about metadata and have a general understanding about how this data can be accessed and interpreted.

In addition, metadata is changing all the time. Some metadata is altered simply by opening a file. For example, data in the "Access" field is changed the instant a file is opened for viewing, printing or simply copying over to another file, with the original data possibly disappearing forever. This trait makes metadata the most fragile of electronic evidence, highly susceptible to loss or alteration by anyone with access. The existence of multiple sets of metadata can also expose discrepancies in the available data that can be an indication of alteration, duplication, or deletion of an electronic file.

Professional Liability Implications of Metadata

Recent amendments to the Federal Rules of Civil Procedure have clarified what is potentially discoverable in litigation to include all "electronically stored information." As this definition is broad enough to include metadata, all metadata is subject to the rules of discovery and the usual duties to preserve and produce. It is therefore important for lawyers to consider metadata in the same way they look at other evidence – in terms of relevance and accessibility.

Metadata also can seriously impact the ethical duties owed by lawyers and the legal obligations of their

clients, thereby exposing lawyers to an array of professional liability risks. Even though metadata is not readily visible to attorneys creating or handling it, its inadvertent disclosure or destruction by lawyers or their clients could provide cause for a disciplinary complaint or claim for legal malpractice. For example, consider the following:

During settlement negotiations, you and your client exchange drafts of a settlement agreement via e-mail, using a typical collaboration feature to insert and exchange comments and edits. When finished, you send a settlement proposal via e-mail to opposing counsel attaching the draft agreement. But, unless this information is cleansed or locked-down in the document prior to transmission, any sensitive confidences or strategies expressed in the editorial comments exchanged with your client can be viewed by opposing counsel by accessing the metadata, thereby potentially compromising your client's bargaining position.

* * *

Your client is ordered to produce its employee file for a terminated employee in a case in which the timing of events is critical. The client sends you the file on a disk for production to the other side. After reviewing the electronic files and documents on the disk for privilege, you deliver the disk to opposing counsel, who subsequently complains to the court that all of the potentially relevant metadata underlying this electronic record evidence has been altered and lost as a result of your access and review.

Under the rules in every jurisdiction, lawyers have ethical duties to maintain client confidences and safeguard client property and information. These duties clearly extend to the protection of client information in digital form. Lawyers using computers and other electronic devices thus have an ethical obligation to become familiar with the basic operation of the media or software used to create, modify, and transmit client data to avoid disclosure or loss of information causing harm to the client. While lawyers don't need to be technology experts, they do need to gain a basic understanding of this information and how it can impact their clients, especially those that are, or likely to become, parties to a civil, criminal or regulatory investigation or suit. In many circumstances, this may mean the lawyer must seek out the assistance of the client's custodian of records and chief information officer, or some other person most familiar with the client's use of technology.

So far, a number of courts have concluded that responsive electronic records produced in discovery must include metadata and be fully searchable. See *Williams v. Sprint/United Management Company*, 230 F.R.D. 640 (2005); *Nova Measuring Instruments, Ltd. v. Nanometrics, Inc.* 417 F. Supp. 2d 1121 (N.D. Cal 2006); *In Re Verisign*, 2004 WL 2445243 (N.D. Cal 2004). In fact, some courts have placed the burden on the responding party to object to the production of metadata and demonstrate why such information should not have to be produced. In *Williams*, the Kansas District Court held that electronic files produced in the form and manner they had been kept by the producing party in the normal course of business must be produced in a usable form with the accompanying metadata intact.

The information contained in metadata can also give rise to concerns about privacy and privilege. In

circumstances where the data is critical to the subject of a negotiation or dispute, safeguarding metadata could be critical to the representation and advancement of the client's interests. The greater the amount of evidence produced in electronic form, the greater the odds that undiscoverable confidential or privileged content will be disclosed in metadata. As lawyers increasingly use e-mail and other means to exchange documents electronically with clients, counsel and the court, the need to manage and control metadata becomes imperative.

The ABA recently determined that lawyers are not prohibited from accessing and viewing metadata embedded in electronic documents or files, even if obtained from an adverse party or opposing counsel. See ABA Formal Op. 06-442 (Aug. 5, 2006) (*Review and Use of Metadata*). It concluded that although Rule 4.4(b) requires a lawyer who receives inadvertently sent information to promptly notify the sender (see ABA Formal Op. 05-437 (October 1, 2005) (*Inadvertent Disclosure of Confidential Materials*) (*withdrawing* Formal Op. 92-368)), the rules say nothing about the receiving lawyer's right to review or use such information, provided it was not unlawfully or unethically obtained.

The ABA's Opinion on metadata actually conflicts with the findings of two state ethics panels which deemed it unethical for attorneys to use technology to "mine" documents surreptitiously for embedded information. See N.Y. State Bar Ass'n Op. 749 (2001); Fla. Bar Ass'n Op. 06-2 (September 16, 2006); *but see* Md. State Bar Ass'n Comm. On Ethics Op., 2007-09 (October 19, 2006). However, both of these states also impose on lawyers a duty to use reasonable care when transmitting documents by e-mail to prevent the disclosure of metadata containing client confidences or secrets. According to the New York Bar, "reasonable care may...call for the lawyer to stay abreast of technological advances and the potential risks in transmission in order to make an appropriate decision with respect to the mode of transmission."

The ethics rules notwithstanding, attorneys cannot prevent savvy clients or third parties from uncovering sensitive metadata. Consequently, while some jurisdictions may protect lawyers from covert access of metadata by another lawyer, attorneys who send documents electronically nevertheless have an affirmative duty to take reasonable precautions to ensure that confidential or other potentially damaging information contained therein is removed prior to transmittal. By implication, an attorney also has a duty to warn clients of such risks.

Managing the Risks Associated with Metadata

Lawyers can help minimize the risks associated with metadata by the following:

- ***Learn what you don't know or understand about metadata.***

Since very few lawyers are technology experts, lawyers should determine the extent of their ignorance about metadata, and electronic data in general. Because the technological capabilities of lawyers varies so widely, each lawyer must assess his own need for education and training about the metadata that accompanies both electronic client records and their own records. Since the proper handling of client and firm metadata and other electronic records involves a considerable amount of technical know-how, for many lawyers this may require engaging a technology consultant or other expert for help in getting started or advice on individual needs and the

best methods and products available.

- ***Advise clients about metadata.***

Similarly, attorneys should survey clients to determine their level of knowledge and understanding about metadata. At the inception of each representation, lawyers should discuss the handling of electronic documents generally and advise clients about the nature and significance of metadata. Procedures for maintaining and managing electronic documents, including metadata, in the event it is needed in the discovery process should be discussed. This should include counsel on controlling and managing the disclosure of potentially harmful metadata and preserving and producing it if required.

- ***Establish policies for dealing with metadata.***

Lawyers and firms should establish policies that account for metadata and its associated risks. Most importantly, lawyers need to exercise caution when exchanging documents electronically. There are certain types of documents and records that should not be transmitted electronically at all, and lawyers should generally avoid sending documents to third parties in their native formats. Instead, all such items should either be converted to a Portable Document Format (PDF) or scanned and converted to a transmittable image, which will remove most, but not all, potentially harmful metadata.

Other policies lawyers should institute include rules and procedures governing the use of e-mail by employees. Given the extent to which e-mail has become a gold mine for incriminating evidence, lawyers need to be increasingly circumspect about when and how they use e-mail to correspond with individuals outside the firm. The old tools of the trade should not be abandoned just because new methods have been introduced; where confidentiality and authenticity are a major concern, documents should be sent via fax machine to a waiting recipient, by messenger or overnight delivery service, or even that old dinosaur, the U.S. Postal Service.

Lastly, every firm or law practice should decide whether it will archive or destroy the metadata corresponding to its internal lawyer and firm records. This is a policy issue that should be addressed in the firm's written record retention policy. Whether metadata will be left untouched or destroyed in the normal course of business is up to the firm, subject to applicable law and ethics rules. Consistency in application by both lawyers and employees is the key. The costs of destroying metadata while safely preserving needed underlying records may outweigh the benefits of destruction, and in the long run such information could be beneficial to the firm in defending against a claim or lawsuit.

- ***Consider a metadata scrubbing application.***

To protect against disclosure of potentially harmful metadata, in addition to using scanning technology and PDF conversion tools, lawyers should consider obtaining a reliable commercial software tool that "scrubs" unwanted metadata. These widely available programs alert users of the existence of metadata and remove it prior to archiving or transmission. In addition to commercial scrubbers, many common document applications now offer

proactive metadata removal tools.

- **Address metadata early in the discovery process.**

Since every electronic file comes with its own autobiography, the question is not whether metadata exists, but where it is, how much there is, and whether it is necessary to unearth it. Moreover, because metadata is changing all the time, the need to avoid compromising the *status quo* of metadata evidence must be addressed as soon as possible at the outset of discovery. Litigators should include metadata in all of their deliberations and discussions with clients and counsel about electronic data to be preserved and produced, including their “meet and confer” discussions required under amended FRCP Rule 34. Under the rules of discovery, litigants usually have the option of producing information and documents in the manner in which they are kept in the ordinary course of business. However, litigants who produce electronic records this way will be expected to produce them in a readable and searchable format. This is particularly important when producing e-mails and attachments, as such files frequently use incompatible software applications that result in unreadable data.

Conclusion

As technology revolutionizes the practice of law, in more and more ways electronic data has replaced paper as a lawyer’s primary stock-in-trade, and lawyers must be ever-conscious of the difference. Failing to consider and account for the existence of metadata within electronic records can result at a minimum in embarrassment, or worse, sanctions, penalties, ethics complaints, and claims of legal malpractice. Lawyers have a duty to handle metadata with the same level of competence and discretion as required with any other form of client information or property. Knowing that metadata exists, where it can be found, and what significance it may have is an essential skill for lawyers to safely practice law in today’s environment.

For more information about metadata and assistance or products available, go to www.metadatarisk.org

January 2007

By: Michael Vahey, J.D., Risk Control Consultant, CNA Lawyers Professional Liability, CNA Center, Chicago, IL

The purpose of this article is to provide information, rather than advice or opinion. It is accurate to the best of the author’s knowledge as of the date of this article. Accordingly, this article should not be viewed as a substitute for the guidance and recommendations of a retained professional. In addition, CNA may not necessarily endorse any coverages, systems, processes or protocols addressed herein unless such coverages, systems, processes or protocols are produced or created by CNA.

References to non-CNA websites or articles are provided solely for convenience, and CNA disclaims any responsibility for their content. To the extent this article contains any examples, please note that they are for illustrative purposes only and any similarity to actual individuals, entities, places or situations is unintentional and purely coincidental. In addition, any examples are not intended to establish any standards of care, to serve as legal advice appropriate for any particular factual situations, or to provide an acknowledgement that any given factual situation is covered under any CNA insurance policy. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All CNA products and services may not be available in all states.

CNA is a service mark registered with the United States Patent and Trademark Office. Copyright © 2007, CNA. All rights reserved.

