WHITE PAPER

Metadata: What Lawyers and Their Legal Support Team Need to Know

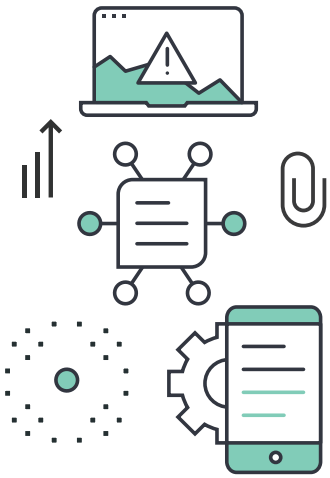
By: Katherine W. Dandy, Esq.

LITERA

This white paper discusses the management of metadata in the e-discovery context. It will address how and when metadata is generated, how it can be accessed, and how it can be removed, with an eye toward making the most of e-discovery, as well as protecting client confidences and reducing the risk of inadvertent disclosure. We will provide technical and legal/ethical guidance on sending, receiving, and preserving metadata in documents, so that when the time comes to produce electronically stored information (ESI), legal support teams can be assured that the metadata contained in the ESI has been properly handled.

Metadata is created in the generation of electronic files. Attorneys and their legal support teams need to be aware that when electronic files are transmitted, the mostly hidden metadata contained therein is transmitted as well, and that recipients of the files will be able to access the metadata. However, actions can be taken to prevent or minimize the risk of inadvertent disclosure of metadata. The easiest way to prevent disclosure of confidential metadata is the installation and implementation of metadata "scrubbing" software, which can remove metadata from documents before they are transmitted.

Another practical tip for preventing the disclosure of confidential information in metadata is to convert documents to PDF files before transmission, rather than sending a Word document. While a PDF will have its own metadata, it will likely be limited to the author who created the PDF and the date/time the document was converted. The PDF will not contain the original word processing software metadata.



Scanning a document (as a PDF or TIFF file) is another way to avoid inadvertent disclosure of confidential metadata. If using "track changes" in documents, the user should always check to ensure that there are no changes that need to be accepted or rejected. Lastly, if the attorney plans to redact privileged material from electronic documents, proper redaction tools must be employed, because the redaction is done by hand, the text underneath may still be viewable if the "search," "copy," or "paste" functions are used.

Importantly, while removing metadata before electronic documents are transmitted will often be required to protect client confidences, the duty of preservation of evidence may include the obligation not to scrub certain metadata. Ethical obligations with respect to preserving metadata is discussed further below.

The basic rules prohibiting the disclosure of confidential information apply equally to confidential information in metadata.

1 New York State Bar Association opinion 782 (Dec. 8, 2004).
2 ABA Model Rule of Professional Conduct 4.4(B) provides that "[a] lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."
3 For those with a multijurisdictional practice, consult the applicable choice of law rules. Most likely, for litigated matters, the jurisdiction in which the matter is being heard will apply, and for other matters, the rules of jurisdiction in which the lawyer's conduct occurred will apply. See, e.g., ABA MRPC Rule 8.5. 4 The sedona conference commentary on ethics & metadata (2013) (hereinafter, "sedona commentary"), at 11-12. The sedona conference, a nonprofit legal policy research and educational organization, has a working group comprised of judges, attorneys, and experts dedicated to resolving Electronic document production issues. In the emerging area of e-discovery, courts are often relying on The sedona principles in resolving disputes over the production of metadata. 5 Id., At 12. 6 American Bar Association Formal Ethics Opinion 06-442 (august 5, 2006).

Ethical Obligations with Respect to Sending and Receiving Metadata

The basic rules prohibiting the disclosure of confidential information apply equally to confidential information in metadata. For example, the New York State Bar Association has stated that lawyers "must exercise reasonable care to prevent the disclosure of confidences and secrets contained in 'metadata' in document [sic] they transmit electronically to opposing counsel or other third parties."[1]

As to receiving metadata, most jurisdictions require a lawyer who receives a file from another lawyer through inadvertence to notify the sending lawyer.[2] Depending on the jurisdiction governing the receiving lawyer's conduct, different duties may apply to a lawyer who receives a file containing metadata sent by another.[3] Several bar associations' ethics opinions prohibit the receiving lawyer's viewing of any of the file's metadata (often referred to as "data mining").

It has been noted, however, that many of the bar association opinions assume incorrectly that all metadata is per se confidential.[4] This misunderstanding of the different types of metadata has led to blanket prohibition on viewing any metadata, even metadata that would have no claim to confidentiality, such as some "application" metadata which, for example, instructs the computer how to display fonts.[5]

Some jurisdictions (Colorado, DC, and West Virginia) generally allow a lawyer to examine a received file for metadata unless the receiving lawyer has actual knowledge that the file contains confidential metadata and should assume that the information was transmitted inadvertently. For example, Maryland, Vermont, and Minnesota have no prohibition on reading metadata received from another. This is also the position of the ABA.[6]

Ethical Obligations with Respect to Preserving Metadata

A lawyer must not unlawfully alter, destroy, or conceal a file or other material having potential evidentiary value.[7] If one reasonably anticipates litigation, one must take care to prevent the routine deletion of certain metadata, especially embedded metadata in potentially relevant ESI.[8] For example, attorneys must not delete metadata such as tracked changes when the changes show the contract negotiations between business people if the contract is the subject of likely litigation.[9] Such deletion may constitute spoliation if a legal duty exists to preserve the data that is being scrubbed.[10] Removing metadata from certain evidentiary files may even be illegal.[11]

Preservation obligations and practices outside the context of reasonably anticipated litigation, however, differ considerably.[12] Absent a legal requirement to the contrary, organizations are not required to retain metadata.[13]

7 See e.g., ABA Model Rules of Professional Conduct, Rule 3.4(a), Fairness to Opposing Party and Counsel ("A lawyer shall not: (a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act. ...")
8 Sedona Commentary, at 9.
9 Id.; see also Williams v. Sprint/ United Mgmt. Co., 230 FRD 640, 653 (D.Kan. 2005) (metadata associated with changes to spreadsheets, dates of changes, identification of individuals making changes, and other metadata from which plaintiffs could determine final versus draft versions of spreadsheets appear relevant and should be produced).
10 Id. Receipt by a party of a litigation hold notice will trigger a duty not to remove metadata.
11 Id.
12 Id.
13 Id.
14 See Williams, supra., at 647.
15 Id.
16 FRCP 34(b)(2)(E)(ii)-(iii).
17 Fed.R.Civ.P. 34, Advisory Committee Note (2006 Amends.).
18 See Harry Weiss, Inc. v. Moskowitz, 106 AD3d 668, 670 (1 Dept. 2013) (preclusion upheld as appropriate sanction where plaintiff converted files from native format to hard copy form).

Guidelines for Seeking Metadata During Discovery

To obtain discovery of metadata, attorneys should request that responsive files be produced "in native format with all metadata intact" or in a "reasonably useable form," which may include specified files of metadata. Where Excel spreadsheets are being sought, the request should be that they be produced as an "active file."

Attorneys must be prepared to support a request for production of metadata with a reasonable basis for same. In arguing that metadata is relevant and should be produced, keep in mind that the more interactive an application is, the more important the metadata will be to understand the application's output.[14] For example, a Word document can generally be understood simply by reading it, without the need for metadata. That said, certain metadata, such as draft revision history and author information, could be highly relevant to the issues in a case, and therefore discoverable. The need for metadata from a spreadsheet will depend on the complexity and purpose of the spreadsheet.[15]

Lastly, caution should be exercised in demanding that ESI be produced in native format with metadata intact, as your adversary may turn around and insist upon the same from you.

Guidelines for Producing Metadata in Discovery

In general, when electronic discovery is requested, such discovery should be produced in an electronic format. Under the Federal Rules of Civil Procedure, if a request does not specify a particular form, the responding party must produce it in a form in which it is "ordinarily maintained," or in a "reasonably usable" form or forms, and "need not produce the same electronically stored information in more than one form."[16] The option to produce in a reasonably usable form, however, does not mean that a responding party is free to convert ESI from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation. For example, if the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature.[17] Indeed, courts have observed that converting files from their "native" format, i.e., how it is stored and used in the normal course of business, to hard-copy form for production would result in the loss of discoverable metadata.[18]

Where a party is ordered to produce electronic documents as they are maintained in the ordinary course of business (or in their "native format," or "as an active file"), the producing party should produce the electronic documents with their metadata intact, unless the party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order.[19] Additionally, in the first instance, a producing party "need not provide discovery of [ESI] from sources that the party identifies as not reasonably accessible because of undue burden or cost."[20]

Practically—and technologically—speaking, if "native" files are requested, it is sufficient to produce electronically stored information in PDF or TIFF format accompanied by a "load" file containing searchable text and selected metadata.[21] Such a production will be in "usable form," meaning electronically searchable and paired with essential metadata."[22]

As for viable objections to the production of metadata, other than certain types of embedded metadata (e.g., tracked changes, presentation notes, or comments), there will be very little metadata for which a claim of privilege can be asserted.[23] If privilege is claimed, the objecting party must produce

19 See Williams, supra., at 652.
20 Aguilar, supra., at 360, quoting FRCP 26(b)(2)(B).
21 See The Sedona Principles, Second Edition: Best Practice Recommendations & Principles for Addressing Electric Document Production (2007), at Principle 12.
22 Id.
23 Sedona Commentary, at 16.
24 Williams, supra., at 653-654.
25 Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L., 2006 WL 665005 (N.D.Ill.)
26 Ky. Speedway, LLC., supra., at 8-9.
27 Williams, supra.., at 654.
28 Aguilar, supra., at 360, quoting FRCP 26(b)(2)(C).
29 Id., at 362.

a privilege log as to deleted metadata, or risk waiving the privilege.[24] A responding party may object to the production of metadata on the basis of relevance. Courts have found metadata to be relevant where it will allow a party to "piece together the chronology of events and figure out, among other things, who received what information and when."[25] A party may be directed to produce metadata for documents for which "date and authorship is unknown but relevant."[26] Keep in mind that if a court finds that the producing party "should reasonably have known" that metadata was relevant, that party may be ordered to produce metadata, even though it was not requested initially.[27]

In ruling on a discovery dispute over metadata, the court will consider the degree to which the discovery sought is "unreasonably cumulative or duplicative" and whether "the burden or expense of the proposed discovery outweighs its likely benefit."[28] Moreover, if metadata was not requested until after ESI was produced in one form, the party making the request may bear the cost of the subsequent production.[29]

Conclusion

While attorneys may not be ready to embrace all new technology, they must keep abreast of relevant changes in technology, just as they do with changes in law. Metadata can be extremely useful in a case, but attorneys have to know how and where to look for it. Similarly, it can be harmful to lawyers and clients if seen by the wrong eyes, so law firms must educate themselves on the available safeguards before transmitting electronic documents. Taking an out-of-sight, out-of-mind approach to metadata is not a wise choice, and can lead to disciplinary violations, and even malpractice. The old adage "knowledge is power" applies with equal force to what may be hidden in your documents! •

LITERA

About us

Litera is the leading provider of software for drafting, proofreading, comparing, repairing, and cleaning documents in the legal and life sciences industries worldwide. Our core products empower users to generate, review, and distribute high quality content quickly and securely, from any device. Today, Litera supports thousands of document-intensive organizations across the globe, helping them satisfy the complex demands of clients and regulators.