

Digital Workflow

Metadata is usually harmless, but not always

What is metadata?

Strictly speaking metadata is ‘data about data,’ of any sort in any media. Of course all data is ‘about something,’ and is therefore metadata. In the context of modern computers metadata usually means information about a computer file other than what was created by the human author(s) of that file. For example, metadata would include file attributes such as name, size, data type, or where it is located, how it is associated, ownership, etc.

In other words metadata is usually file information that is created by a computer at the same time that a human being is creating the information that will be contained in the file.

Why is metadata considered bad?

Ordinarily metadata isn’t bad. But when people attempt to hide the fact that a file has been altered in a certain way those people consider metadata bad because it thwarts that effort. Sometimes people want to keep certain facts confidential, and with legitimate reason. In that case, metadata might be problematic if it could be easily examined by anyone with access to the file. Usually, though, nobody cares if someone else can see who created their document, or when it was created.

Tracking changes in word processing documents

When a computer keeps track of changes to a word processing document the resulting record of changes can be considered ‘metadata.’ This type of metadata is by far the greatest threat to most attorneys.

The solution to ‘bad metadata’

Obviously the solution is to get rid of risky metadata, but how? Generally speaking the solution for text based documents (e.g. Word or WordPerfect documents) is to convert them to PDF before sending them out. However, since the method for creating PDFs from Word or WordPerfect generally involves capturing a ‘phantom print job,’ anything that would be revealed in that print job would wind up as visible text in the PDF. So, if you had your preferences set to print out ‘tracked changes’ then the PDF would show the changes. But this wouldn’t be metadata; it would be worse: it would be plainly visible on the page.

If you are a transactional attorney, or if you simply must exchange native files with someone outside your office, then you should consider getting a program that scrubs out metadata. There are several types of programs in this category to meet the needs of small firms as well as large firms. For small firms using Microsoft Word the built-in Document Inspector will usually get the job done. Another product to try is by the Payne Consulting

Group's [Metadata Assistant](#), which removes metadata from Word, Excel and PowerPoint files.

Convert to PDF

As we said, the best policy is generally to convert text documents (or spreadsheets and Powerpoint documents) to PDF, if possible. Unless it's absolutely necessary to share the native file this is the safest method. Just remember to examine the resulting PDF to see if you accidentally included tracked changes, and that it's otherwise devoid of any serious problems. The nice thing about PDFs is that any serious problems will be visible right on the page.

Ethics of examining metadata

Bar associations are starting to examine the question of whether and when it might be permissible to purposefully look at an opposing attorney's metadata. The ABA adopted a position that it was permissible to examine metadata, but New York and Alabama have taken opposing views. We have attached the ABA provision (06-442) and the Alabama provision (which cites and discusses the New York rule), along with a brief article.

Louisiana, has not taken a position on this subject as yet.

Fujitsu ScanSnap S510
FUJITSU



With easy-to-use
"one-touch" features

\$461^{99*}

*\$50 mail-in rebate available;
offer ends 12/31

[Learn More ▶](#)



[Home](#) » [News](#) » New Legal Ethics Minefield: Metadata

Science & Technology Law

New Legal Ethics Minefield: Metadata

Posted Feb 20, 2008, 03:44 pm CST

By [Martha Neil](#)

Have you eliminated all metadata from electronic documents you send to opposing counsel? Do you look for metadata in the documents you receive? And, in both cases, does your approach, whatever it is, comply with applicable legal ethics standards?

The correct answers to those questions aren't necessarily clear, but a growing body of case law is developing to address them, reports the [National Law Journal](#).

"When I first gave a lecture on metadata four years ago, there was only [a] New York ethics opinion," says Andrew Perlman of Suffolk University Law School. "In the last year, there has been four or five more. In the next three to four years, I expect we will see an explosion of opinions. This is just beginning."

Along with sending a privileged fax to the wrong party and failing to hang up the speakerphone before a confidential conversation begins, lawyers—and their support staff—need to be careful not to e-mail computerized documents or send disks that contain earlier versions of the document that a computer expert can readily read, the legal publication explains. But many don't even realize that transmitting metadata is an issue, let alone how it should be addressed.

Even sophisticated law firms can easily make mistakes with metadata, says David Hricik of Mercer University's Walter F. George School of Law. He tells a cautionary tale, for instance, of a Word document posted online that allowed a sophisticated user, with two clicks, to determine from an earlier draft that the plaintiff had originally intended to sue a different defendant. Redacted documents produced in discovery can also pose major problems, if metadata hasn't been fully eliminated.

Meanwhile, those who are well-aware of the issue can potentially gain a litigation advantage by discovering the original electronic version of the document, including its metadata.

For more information about the metadata minefield and ideas about how to ethically navigate it, read this [ABA Journal](#) article.

Commenting has expired on this post.

Copyright 2008 American Bar Association. All rights reserved.

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 06-442

August 5, 2006

Review and Use of Metadata

The Model Rules of Professional Conduct do not contain any specific prohibition against a lawyer's reviewing and using embedded information in electronic documents, whether received from opposing counsel, an adverse party, or an agent of an adverse party. A lawyer who is concerned about the possibility of sending, producing, or providing to opposing counsel a document that contains or might contain metadata, or who wishes to take some action to reduce or remove the potentially harmful consequences of its dissemination, may be able to limit the likelihood of its transmission by "scrubbing" metadata from documents or by sending a different version of the document without the embedded information.

In modern legal practice, lawyers regularly receive e-mail, sometimes with attachments such as proposed contracts, from opposing counsel and other parties. Lawyers also routinely receive electronic documents that have been made available by opponents, such as archived e-mail and other documents relevant to potential transactions or to past events. Receipt may occur in the course of negotiation, due diligence review, litigation, investigations, and other circumstances.

E-mail and other electronic documents often contain "embedded" information. Such embedded information is commonly referred to as "metadata."¹ This opinion² addresses whether the ABA Model Rules of Professional Conduct permit a lawyer to review and use embedded information contained in e-mail and other electronic documents, whether received from opposing counsel, an adverse party³ or an agent of an adverse party. The Committee

1. Creation of metadata is not a new phenomenon. For example, for decades, documents saved on personal computers typically have contained embedded information recording the last date and time that the documents were saved.

2. This opinion is based on the Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2003. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in the individual jurisdictions are controlling.

3. This opinion assumes that the receiving lawyer did not obtain the electronic documents in a manner that was criminal, fraudulent, deceitful, or otherwise improper, for example, by making a false statement of material fact to opposing counsel or to any other third person (Model Rule 4.1(a)), using a method of obtaining evidence that violated the legal rights of a third person (Model Rule 4.4(a)), or otherwise engaging in misconduct (Model Rule 8.4). Such scenarios are beyond the scope of this opinion.

AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY, 321 N. Clark Street, Chicago, Illinois 60610-4714 Telephone (312)988-5300 CHAIR: William B. Dunn, Detroit, MI □ Elizabeth Alston, Mandeville, LA □ T. Maxfield Bahner, Chattanooga, TN □ Amie L. Clifford, Columbia, SC □ Timothy J. Dacey, III, Boston, MA □ James A. Kawachika, Honolulu, HI □ Steven C. Krane, New York, NY □ John P. Ratnaswamy, Chicago, IL □ Irma Russell, Memphis, TN □ Thomas Spahn, McLean, VA □ CENTER FOR PROFESSIONAL RESPONSIBILITY: George A. Kuhlman, Ethics Counsel; Eileen B. Libby, Associate Ethics Counsel

© 2006 by the American Bar Association. All rights reserved.

concludes that the Rules generally permit a lawyer to do so.⁴

Metadata is ubiquitous in electronic documents. For example:

- Electronic documents routinely contain as embedded information the last date and time that a document was saved, and data on when it last was accessed. Anyone who has an electronic copy of such a document usually can “right click” on it with a computer mouse (or equivalent) to see that information.
- Many computer programs automatically embed in an electronic document the name of the owner of the computer that created the document, the date and time of its creation, and the name of the person who last saved the document.⁵ Again, that information might simply be a “right click” away.
- Some word processing programs allow users, when they review and edit a document, to “redline” the changes they make in the document to identify what they added and deleted. The redlined changes might be readily visible, or they might be hidden, but even in the latter case, they often will be revealed simply by clicking on a software icon in the program.
- Some programs also allow users to embed comments in a document. The comments may or may not be flagged in some manner, and they may or may not “pop up” as a cursor is moved over their locations.

Other types of metadata may or may not be as well known and easily understandable as the foregoing examples. Moreover, more thorough or extraordinary investigative measures sometimes might permit the retrieval of embedded information that the provider of electronic documents either did not know existed, or thought was deleted.

4. Comment [16] to Model Rule 1.6 states, “[a] lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1, and 5.3.” Addressing whether the sending or producing lawyer acted competently in any given factual scenario is beyond the scope of this opinion. *See also* New York State Bar Ass’n Committee on Prof’l Eth. Op. 782 (Dec. 8, 2004), (E-mailing documents that may contain hidden data reflecting client confidences and secrets), available at http://www.nysba.org/Content/NavigationMenu/Attorney_Resources/Ethics_Opinions/Opinion_782.htm (last visited Sep. 15, 2006) (under New York’s Code of Professional Responsibility, New York’s version of predecessor ABA Model Code of Professional Responsibility, lawyers must exercise reasonable care to prevent inappropriate disclosure of client confidences and secrets contained in metadata).

5. The names generally are automatically derived from the name of the owner of the computer on which the document is created or from the name associated with the user identification of the person who accessed the computer program. If a document is copied and altered, it still might contain the name of the creator of the original document. Thus, the embedded information about the creator of a document or who last saved it might or might not identify the person(s) who actually created or saved it.

Not all metadata, it should be noted, is of any consequence; most is probably of no import. In ordinary day-to-day circumstances, the embedded information that is found in most documents, such as when they were saved, or who the authors were, is unlikely to be of any interest, much less material to a matter. In some instances, however, such as when a party to a lawsuit is attempting to establish “who knew what when,” the date and time that a critical document was created or who drafted it may be a critical piece of information. If a payment amount is being negotiated, then a redlined change or a comment in a draft agreement that suggests how much more the opposing party is willing to pay or how much less they might take likely is of the highest importance.

The Committee first notes that the Rules do not contain any specific prohibition against a lawyer’s reviewing and using embedded information in electronic documents.⁶ The most closely applicable rule, Rule 4.4(b), relates to a lawyer’s receipt of inadvertently sent information. Even if transmission of “metadata” were to be regarded as inadvertent,⁷ Rule 4.4(b) is silent as to the ethical propriety of a lawyer’s review or use of such information. The Rule provides only 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.”⁸ Comment [3] to Model Rule 4.4 indicates that, unless other law requires otherwise, a lawyer who receives an inadvertently sent document ordinarily may, but is not required to, return it unread, as a matter of professional judgment.⁹

6. As stated earlier, this opinion assumes that the receiving lawyer acted lawfully and ethically in obtaining the electronic documents.

7. The Committee does not characterize the transmittal of metadata either as inadvertent or as advertent, but observes that the subject may be fact specific. As noted in Formal Opinion 06-440 (May 13, 2006) (Unsolicited Receipt of Privileged or Confidential Materials: Withdrawal of Formal Opinion 94-382 (July 5, 1994)), there is no Model Rule that addresses the duty of a recipient of advertently transmitted information.

8. Comment [2] to Rule 4.4 confirms that the word “document” includes e-mail and other electronic documents. The Comment also indicates that the notification requirement exists “in order to permit [the sender] to take protective measures,” and includes a recognition that applicable other law (outside of the applicable rules of professional conduct) may require the lawyer to take additional steps beyond notification.

9. Rule 4.4(b) was added to the Model Rules in 2002. The clarity of its requirements provided the basis for the Committee to withdraw two of its past formal ethics opinions. First, the Committee, in Formal Opinion 05-437 (Oct. 1, 2005) (Inadvertent Disclosure of Confidential Materials: Withdrawal of Formal Opinion 92-368 (Nov. 10, 1992)), withdrew its Formal Opinion 92-368 (Nov. 10, 1992) (Inadvertent Disclosure of Confidential Materials). Formal Opinion 92-368 opined that a lawyer who receives materials that on their face appear to be subject to the attorney-client privilege or otherwise confidential under Model Rule 1.6, under circumstances where it is clear they were not intended for the receiving lawyer, should refrain from examining the materials, notify the sending lawyer, and abide by the instructions of the sending lawyer. Second, the Committee, in Formal Opinion 06-440 (May 13, 2006) (Unsolicited

Some authorities have addressed questions related to a lawyer's search for, or use of, metadata under the rubric of a lawyer's honesty, and have found such conduct ethically impermissible.¹⁰ The Committee does not share such a view, but instead reads the recent addition of Rule 4.4(b) identifying the sole requirement of providing notice to the sender of the receipt of inadvertently sent information, as evidence of the intention to set no other specific restrictions on the receiving lawyer's conduct found in other Rules.¹¹ Whether the receiving lawyer knows or reasonably should know that opposing counsel's sending, producing, or otherwise making available an electronic document that contains metadata was "inadvertent" within the meaning of Rule 4.4(b), and is thereby obligated to provide notice of its receipt to the sender, is a subject that is outside the scope of this opinion.¹²

The Committee observes that counsel sending or producing electronic doc-

Receipt of Privileged or Confidential Materials: Withdrawal of Formal Opinion 94-382 (July 5, 1994)), withdrew its Formal Opinion 94-382 (July 5, 1994) (Unsolicited Receipt of Privileged or Confidential Materials). Formal Opinion 94-382 addressed the obligations under the Rules of a lawyer who is offered, or is provided, by a person not authorized to offer them, materials of an adverse party that the lawyer knows to be, or on their face appear to be, subject to the attorney-client privilege or otherwise confidential under Rule 1.6.

10. The Committee notes that New York State Bar Ass'n Committee on Prof'l Eth. Op. 749 (Dec. 14, 2001) (Use of computer software to surreptitiously examine and trace e-mail and other electronic documents), available at http://www.nysba.org/Content/NavigationMenu/Attorney_Resources/Ethics_Opinions/Committee_on_Professional_Ethics_Opinion_749.htm (last visited Sept. 15, 2006) took the position that under New York's Code of Professional Responsibility, a lawyer may not "intentional[ly] use ... computer technology to surreptitiously obtain privileged or otherwise confidential information" of an opposing party. The New York committee reaffirmed that view in the opinion cited in footnote 4, *supra*. The Committee recognizes that Opinion 749 relies in part on language contained in present Rule 8.4(c) and (d) that prohibits engaging in conduct "involving dishonesty, fraud, deceit, or misrepresentation" or "that is prejudicial to the administration of justice." However, the Committee does not believe that a lawyer, by acting within the circumstances assumed by the instant opinion, would violate either of those paragraphs of Rule 8.4. The Committee views similarly an opinion issued for comment at the request of the Florida Bar Board of Governors by the Florida Bar Professional Ethics Committee. See Proposed Adv. Op. 06-02 (June 23, 2006), available at [http://www.floridabar.org/TFB/TFBResources.nsf/Attachments/53EDED5599019138525719A006DCE1B/\\$FILE/062%20pao.pdf?OpenElement#search=%22Florida%20%2B%20opinion%20%2B%20metadata%22](http://www.floridabar.org/TFB/TFBResources.nsf/Attachments/53EDED5599019138525719A006DCE1B/$FILE/062%20pao.pdf?OpenElement#search=%22Florida%20%2B%20opinion%20%2B%20metadata%22) (last visited Sept. 15, 2006).

11. We note that this interpretation was intended by the Commission on Evaluation of the Rules of Professional Conduct ("Ethics 2000 Commission"), as reported in the Reporter's Explanation of Changes, available at <http://www.abanet.org/cpr/e2k/e2k-rule44rem.html> (last visited Sept. 15, 2006), regarding this amendment.

12. One of the facts that might be relevant is whether the metadata is a privileged communication.

uments may be able to limit the likelihood of transmitting metadata in electronic documents. Computer users can avoid creating some kinds of metadata in electronic documents in the first place. For example, they often can choose not to use the redlining function of a word processing program or not to embed comments in a document. Simply deleting comments might be effective to eliminate them. Computer users also can eliminate or “scrub” some kinds of embedded information in an electronic document before sending, producing, or providing it to others.¹³ Methods to avoid or eliminate embedded information have been, and no doubt will continue to be, discussed in many legal programs, practice guides, and articles,¹⁴ as well as in general office software publications and support web sites. The specifics of any such software are beyond the scope of this opinion.

A lawyer who is concerned about the possibility of sending, producing, or providing to opposing counsel a document that contains or might contain metadata also may be able to send a different version of the document without the embedded information. For example, she might send it in hard copy, create an image of the document and send only the image (this can be done by printing and scanning), or print it out and send it via facsimile.

Finally, if a lawyer is concerned about risks relating to metadata and wishes to take some action to reduce or remove the potentially harmful consequences of its dissemination, then before sending, producing, or otherwise making available any electronic documents, she may seek to negotiate a confidentiality agreement or, if in litigation, a protective order, that will allow her or her client to “pull back,” or prevent the introduction of evidence based upon, the document that contains that embedded information or the information itself.¹⁵ Of course, if the embedded information is on a subject such as her client’s willingness to settle at a particular price, then there might be no way to “pull back” that information.

13. Of course, when responding to discovery, a lawyer must not alter a document when it would be unlawful or unethical to do so, e.g., Rule 3.4(a) (“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[.]”)

14. For example, the 2006 ABA Techshow included a roundtable program on metadata, and a number of publications and items available on ABA web site pages of the ABA General Practice, Solo & Small Firm Division and the ABA Law Practice Management Section have addressed metadata from practical and ethical perspectives.

15. On April 12, 2006, the Supreme Court of the United States approved extensive amendments to the Federal Rules of Civil Procedure relating to discovery of electronic documents, available at <http://www.uscourts.gov/rules/newrules6.html#cv0804> (last visited September 15, 2006). Among other provisions, certain of the amendments allow a producing party to pull back privileged information and work product under certain circumstances. The amendments will be effective on December 1, 2006, unless Congress enacts legislation to reject, modify, or defer them.

Ethical Propriety of Mining Metadata

DISCLOSURE AND MINING OF METADATA

QUESTION #1:

Does an attorney have an affirmative duty to take reasonable precautions to ensure that confidential metadata is properly protected from inadvertent or inappropriate production via an electronic document before it is transmitted?

ANSWER:

Lawyers have a duty under Rule 1.6 to use reasonable care when transmitting electronic documents to prevent the disclosure of metadata containing client confidences or secrets.

QUESTION #2: Is it unethical for an attorney to mine metadata from an electronic document he or she receives from another party?

ANSWER:

Absent express authorization from a court, it is ethically impermissible for an attorney to mine metadata from an electronic document he or she inadvertently or improperly receives from another party.

DISCUSSION:

The recent proliferation of electronic discovery, e-filing, and use of e-mail has created an ethical dilemma surrounding the disclosure and mining of metadata. For the purposes of this Opinion, metadata may be loosely defined as data hidden in documents that is generated during the creation of those documents. Metadata is most often generated by software programs, such as Microsoft Word and Corel WordPerfect. These programs are frequently used by attorneys in the creation and drafting of legal documents.

The act of deliberately seeking out and viewing metadata embedded in a document is most often referred to as "mining" the document. Mining metadata allows a person to learn a variety of information about the history and evolution of an electronic document, including: the author, the name of previous document authors, template information, and hidden text. By mining an electronic document, a recipient attorney could also view revisions made to the document, comments added by other users that reviewed the document, and whether the document was drafted from a template. The disclosure of metadata contained in an electronic submission to an opposing party could lead to the disclosure of client confidences and secrets, litigation strategy, editorial comments, legal issues raised by the client, and other confidential information.

For example, say your firm is filing a motion to summarily dismiss a lawsuit and the motion is electronically distributed among the firm's attorneys for review and comments. In reviewing the motion, the other attorneys insert comments critiquing the firm's position and discussing the strengths and weaknesses of various legal positions. The motion is then electronically transmitted to opposing counsel. If you failed to "scrub" or remove the hidden metadata prior to transmission, the opposing party could mine the document's metadata and discover which attorneys reviewed the motion, the critiques about the viability or strength of certain arguments, and the subsequent revisions made to the document.

Another example demonstrating the inherent danger of electronically transmitting documents involves the use of templates. Many attorneys routinely recycle templates for common filings, in which the current client's name is substituted in place of a prior client's name. If the document is later electronically transmitted to the opposing party, the opposing party could mine the document and discover the original client's name and information. Such disclosure of client identity and information could constitute a violation of Rule 1.6, Alabama Rules of Professional Conduct. The protection of the confidences and secrets of a client are among the most significant obligations imposed on a lawyer. Rule 1.6, Ala. R. Prof. C., provides that:

"(a) A lawyer shall not reveal information relating to representation of a client unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraph (b)."

The Comment to Rule 1.6, Ala. R. Prof. C., states, in pertinent part:

"The observance of the ethical obligation of a lawyer to hold inviolate confidential information of the client not only facilitates the full development of facts essential to proper representation of the client but also encourages people to seek early legal assistance.

Almost without exception, clients come to lawyers in order to determine what their rights are and what is, in the maze of laws and regulations, deemed to be legal and correct. The common law recognizes that the client's confidences must be protected from disclosure. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is upheld.

A fundamental principle in the client-lawyer relationship is that the lawyer maintains confidentiality of information relating to the representation. The client is thereby encouraged to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter."

As such, the Commission believes that an attorney has an ethical duty to exercise reasonable care when transmitting electronic documents to ensure that he or she does not disclose his or her client's secrets and confidences.

The determination of whether an attorney exercised reasonable care will, of course, vary according to the circumstances of each individual case. Factors in determining whether reasonable care was exercised may include steps taken by the attorney to prevent the disclosure of metadata, the nature and scope of the metadata revealed, the subject matter of the document, and the intended recipient. For example, an attorney would need to exercise greater care in submitting an electronic document to an opposing party than he or she would if e-filing a pleading with the court. There is simply a much higher likelihood that an adverse party would attempt to mine metadata, than a neutral and detached court.

Just as a sending lawyer has an ethical obligation to reasonably protect the confidences of a client, the receiving lawyer also has an ethical obligation to refrain from mining an electronic document. In N.Y. State Bar Opinion 749, the New York State Bar concluded that the use of computer technology to access client confidences and secrets revealed in metadata constitutes "an impermissible intrusion on the attorney-client relationship in violation of the Code." (2001). The Commission agrees that the use of computer technology in the manner described above constitutes an impermissible intrusion on the attorney-client relationship in violation of the Alabama Rules of Professional Conduct. As discussed earlier, the protection of the confidences and secrets of a client is a fundamental tenet of the legal profession.

The unauthorized mining of metadata by an attorney to uncover confidential information would be a violation of the Alabama Rules of Professional Conduct. Rule 8.4, Ala. R. Prof. C., provides that it is misconduct for an attorney to, among other things:

"(a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another;

(b) commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness or fitness as a lawyer in other respects;

(c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation;

(d) engage in conduct that is prejudicial to the administration of justice;"

In Formal Opinion 749, the New York State Bar adroitly observed that "in light of the strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship, use of technology to surreptitiously obtain information that may be protected by the attorney-client privilege, the work product doctrine or that may otherwise constitute a 'secret' of another lawyer's client would violate the letter and spirit of these Disciplinary Rules." (2001) The Disciplinary Commission agrees. The mining of metadata constitutes a knowing and deliberate attempt by the recipient attorney to acquire confidential and privileged information in order to obtain an unfair advantage against an opposing party.

One possible exception to the prohibition against the mining of metadata involves electronic discovery. Recent court decisions indicate that parties may be sanctioned for failing to provide metadata along with electronic discovery submissions. In certain cases, metadata evidence may be relevant and material to the issues at hand. For example, the mining of an email may be vital in determining the original author, who all received a copy of the email, and when the email was viewed by the recipient. In Enron type litigation, the mining of metadata may be a valuable tool in tracking the history of accounting decisions and financial transactions.

The production of metadata during discovery will ordinarily be a legal matter within the sole discretion of the courts. The Commission advises attorneys, however, to be cognizant of the issue of disclosing metadata during discovery. Both parties should seek direction from the court in determining whether a document's metadata is to be produced during discovery.

This opinion is consistent with Formal Opinions 749 and 782 of the New York State Bar and some of the language herein is derived from that opinion.

JWM/s

3/14/07

Click your browser's **BACK** button to continue...

415 Dexter Avenue • Montgomery, Alabama 36104 • (334) 269-1515 • (334) 261-6310 Fax

Copyright © 2008, Alabama State Bar. [Disclaimer](#) (49) 

