ETHICS OPINION

RO-2007-02

OFFICE OF GENERAL COUNSEL

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.[1] Metadata is most often generated by software programs, such as Microsoft Word and Corel WordPerfect.[2] 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.[3] 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.[4]

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.[5] 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

---

[1] Metadata is literally defined as "data about data". Wikipedia contributors (2006). Metadata. *Wikipedia, The Free Encyclopedia*.
[2] David Hricik and Robert Juneman, *The Transmission and Reciept of Invisible Confidential Information*, 15 No. 1 PROF. LAW 18 (2004).
[3] Brian D. Zall , *Metadata: Hidden Information in Microsoft Documents and Its Ethical Implications*, 33 The Colorado Lawyer 83 (October 2004)
[4] Shawn Newman, Comment, *Metadata: Reflection on an Attorney's Professional Responsibility*, WIDENER UNIVERSITY SCHOOL OF LAW (2005).
[5] See *Williams v. Sprint/United Mgmt. Co*., 2005 WL 2401626 (D. Kan. 2005); *In re Telxon Corp. Sec. Litig.*, 2004 WL 3192729 (N.D. Ohio 2004)