ETHICS OPINION NO. 259
OF THE MISSISSIPPI BAR
RENDERED NOVEMBER 29, 2012

CONFIDENTIALITY OF INFORMATION--Metadata-1) An attorney must take reasonable precautions to make sure that confidential metadata is not inadvertently revealed by an electronic document. 2) An attorney may not actively search for confidential metadata in an electronic document received from another attorney.

WARNING: This opinion is limited strictly to the facts set forth in the hypothetical submitted and is limited to the question of whether the proposed conduct is permissible under the MISSISSIPPI RULES OF PROFESSIONAL CONDUCT. The Ethics Committee is prohibited from rendering opinions on questions of law by Article 8-15(c) of the BYLAWS OF THE MISSISSIPPI BAR. Any incidental reference to legal authorities is informational only and should not be taken as the Committee's interpretation of such authorities or of the legal issues arising from the hypothetical presented or of the legal ramifications of the proposed conduct. The Committee's opinion is limited to ethical issues only.

The Ethics Committee has been asked to render an opinion on the following questions:

> 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 by an electronic document before it is transmitted?
> 2. Is it unethical for an attorney to mine meta data from an electronic document he or she receives from another party?

Before answering the preceding two questions, the Committee wants to make clear that the following opinion deals with electronic documents which are voluntarily provided by one attorney to another attorney. Metadata contained in electronic documents provided in response to discovery requests or pursuant to a subpoena are not covered by this opinion and are subject to applicable court rules. For example, the December 1, 2006, amendments to the Federal Rules of Civil Procedure, which introduce the concept of "Electronically Stored Information" (or ESI) specifically deal with the production of electronically stored information in its native format, which contains all metadata related to the ESI. The amendments to the Rules, as well

as numerous court decisions, clearly provide that, in the discovery context, all metadata can be examined (or "mined") for all relevant information, including confidential information.

Definition of Technical Terms

Before answering the questions, the Committee must define the technical terms presented in the questions. There are three which are relevant:

1. What is an *"electronic document"?*

BusinessDictionary.com defines an electronic document as *"information recorded in* a *manner that requires* a *computer or other electronic device to display, interpret, or process it. This includes documents (whether text, graphics, or spreadsheets) generated by* a *software and stored on magnetic media (disks) or optical media (CDs, DVDs), as well as electronic mail and documents transmitted in electronic data interchange (EDI). II* In the legal profession, electronic documents are frequently sent via e-mail, usually as attachments to e-mail. The document may be in Microsoft Word, Corel WordPerfect, Adobe Acrobat, or some other format capable of being read by the receiving party. It is the intention of the Committee to include within this definition, electronically stored information (ESI), which the Sedona Conference has defined as *"electronically stored information, regardless of the media or whether it is in the original format in which it was created, as opposed to stored in hard copy (i.e., on paper)."* The Sedona Conference® Glossary: E Discovery & Digital Information Management, 2nd Edition, December 2007.

2. What is "metadata"?

Almost all electronic documents include data that is not readily visible when viewed on a computer screen or as a printed document. This hidden data is called "metadata." This hidden data provides such mundane information as typeface, font size, italics, bold face, document creation date, names of authors, and other similar information about the document. However, metadata also may include user comments, previous drafts of the document, and deleted text.

3. What is "mining metadata"?

While there is no universally-accepted definition of "mining metadata", the term is defined herein as the act of intentionally seeking out and viewing metadata embedded in a document through the use of software other than the native software application with which the document was created or a native operating system for the purpose of

seeking discovery of information that is confidential, legally privileged, or otherwise not intended to be disclosed on the face of the document.

The Committee distinguishes this definition of "mining metadata" from other, less surreptitious uses of metadata, such as observing readily apparent metadata information like a file creation date of the document, or the use of the "track changes" features built into word processing programs that enable lawyers to collaborate on a document or project. For purposes of this opinion, such innocuous uses of metadata will not be considered "mining metadata", and will instead be referred to as "passive use of metadata."

Thus, the term "mining metadata" as used herein describes the act of actively searching for information that the document sender did not intend for the document recipient to see.

Questions Answered

Having defined the terms as used herein, the Committee now considers the specific questions asked:

> **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?**

Under the Mississippi Rules of Professional Conduct ("MRPC"), a lawyer has an ethical obligation to protect client confidentiality. Specifically, Rule 1.6 (a) provides that "a lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by paragraph (b)."

The Committee, therefore, finds that an attorney has an affirmative duty to take reasonable precautions to ensure that confidential metadata is not inadvertently revealed by an electronic document. No new duty for lawyers to protect client confidentiality is created by this Opinion. However, due to the technological advances, a new category of confidential information which is subject to Rule 1.6, MRPC, exists.

Metadata which attaches to every electronic file can be ascertained by recipients. Some of that information is generic and not confidential. Conversely, some information is potentially confidential. Any confidential information contained

within the metadata is subject to the provisions of Rule 1.6, MRPC, requiring an attorney to protect a client's confidential information.

A review of ethics opinions from around the nation reveals that 17 states have answered this question in the affirmative.[1] Every state which has rendered a formal ethics opinion on this issue has concluded that lawyers have an obligation to understand the technology that they utilize and a lawyer sending files in an electronic format must exercise reasonable care in transmitting files in electronic format so as not to disclose client confidences.

The Committee notes that an attorney has many ways to protect confidential metadata. For example, the attorney may use specialized software which will remove metadata from a file before it is transmitted. (Such acts of removal through software are commonly referred to as "scrubbing" a file.) An even easier way to protect confidential metadata would be to send documents in a PDF format, which may be done by converting the electronic document to a read-only PDF or by printing the document on paper and then scanning it as a PDF document.

2. Is it unethical for an attorney to mine metadata from an electronic document the attorney receives from another party?

Rule 8.4 of the MRPC states in part that:

> It is professional misconduct for a lawyer to:
>
> * * *
>
> (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation;
>
> (d) engage in conduct that is prejudicial to the administration of justice.

The Preamble of the MRPC states, in part: "A lawyer is a representative of clients, an officer of the legal system, and a public citizen having special responsibility for the quality of justice."

Based on these principles, the Committee is of the opinion that it is unethical for an

---

[1] Ala. Formal Op. 2007-02; Ariz. Ethics Op. 07-03; Col. Ethics Op. 119; Fla. Ethics Op. 06-02; Maine Opinion 196; Md. Ethics Doc. 2007-09; Minn. Op. 22; N.H. Op. 2008-2009/4; N.Y. Formal Op. 2003-04; Op. 749, Op. 749, Op. 782; N.C. 2009 Formal Ethics Op. 1; Or. Formal Op. 2011-187; Penn. Formal Op. 2009-100; Vt. Ethics Op. 2009-1; Wash. Advisory Op. 2216 (2012); D.C. Op. 341; W.V. L.E.O. 2009-01; Wis. Ethics Op. EF-12-01.

attorney to mine metadata (i.e., actively search for confidential metadata) from an electronic document which the attorney receives from another party.

Mining for metadata involves the attorney actively looking for confidential metadata. The Committee finds that mining metadata is analogous to an attorney searching an opponent's unattended briefcase during a deposition break or using a listening device when an opposing attorney confers with his client in an adjoining room. The Committee believes that such actions are prejudicial to the administration of justice and are prohibited by the MRPC.

The Committee does not believe that the MRPC prohibit lawyers from passive use of metadata. Such a prohibition would make every lawyer who viewed a file in Windows file manager using the "detail" view unethical, because the lawyer would be able to view the document's creation date or its most recent access date.

Moreover, there are valid reasons why viewing some metadata should be permitted. For example, a lawyer in possession of multiple drafts of a document wanting to determine the most recent version should not be prohibited from sorting the files by creation or modification date, which may be done by a simple click of a mouse when viewed using the "details" view in the operating system. Similarly, lawyers collaborating on the language of a single document, such as a final settlement and release or a commercial loan agreement, should not be prohibited from using the "track changes" features contained in all modern word processing programs in order to propose, accept, and reject language to arrive at a final agreement. (The very purpose of such features is to allow parties to address only proposed changes in a document, and not to have to review the document line by line each time the document is exchanged.) A third example of common passive use of metadata would be observing formulas contained in spreadsheets such as Excel. A lawyer should not be prohibited from looking at the primary input line, simply because the lawyer may discover the formula used to arrive at a number contained in a spreadsheet's cell. (Indeed, a lawyer's obligation to represent his client competently under Rule 1.1 of the MRPC may require the lawyer to have an understanding of how such a number was computed.)

While all three of the preceding examples involve the use of metadata and while ethics committees in other jurisdictions have not drawn a distinction between active and passive use of metadata, this Committee finds that such a distinction should be drawn in order to have the best and most reasonable rule on the ethical use of metadata.

Conclusion

As defined herein, an attorney must take reasonable precautions to make sure that confidential metadata is not inadvertently revealed in an electronic document and an attorney may not actively mine for confidential metadata in an electronic document received from another attorney.