

New Jersey Law Journal

VOL. CXCIV - NO.7 - INDEX 682

NOVEMBER 17, 2008

ESTABLISHED 1878

IN PRACTICE

LEGAL PROFESSION

The Ethical Dilemma of Metadata

Become familiar with this developing and contradicting body of law

BY KENNETH R. MEYER, GENEVIEVE SPIRES
AND JOSEPH A. MANZO

By producing an electronic document in discovery, you may breach the attorney-client privilege, according to an ethics opinion regarding metadata issued by the District of Columbia Bar. That opinion is one of a handful of ethics opinions regarding metadata that have been decided nationwide. Attorneys must familiarize themselves with this developing and sometimes contradictory body of law to avoid potential ethics violations and ensure they protect their clients.

Metadata Defined

Metadata is information hidden in certain types of electronic documents and is automatically generated by document processing and spreadsheet programs. It includes information regarding the creation and revision of electronic documents, including the name of the document's authors, the amount of time spent drafting the document, and hidden text comments. Deliberately searching for and viewing metadata is known as "mining." Mining can be as simple as viewing

Meyer is a principal and Spires is an associate and Manzo is a former associate with Porzio, Bromberg & Newman in Morristown.

a document's properties or as sophisticated as viewing the document with special software designed for that purpose.

While much metadata may be unimportant, certain metadata, like comments made during the revision process, can include attorney-client communications and other protected information. For example, associates often draft answers to interrogatories and then have comments or changes made electronically by both a partner and the client. The original draft answers and subsequent comments may contain privileged or confidential information. Although the electronically transmitted final answers would be "clean" on their face, the metadata contained in the electronic copy could reveal that information.

Thus, metadata can prove to be invaluable evidence. Metadata was used to capture Dennis Rader, the infamous "BTK" serial killer. Rader sent the police anonymous letters in electronic format regarding murders he committed. The metadata in the letters led police to discover Rader's identity, which resulted in his arrest and conviction.

Metadata Best Practices

Production of metadata contained in a document can be intentional or unintentional. Metadata is intentionally produced when parties must provide documents in their electronic form (including

all metadata). In these situations, electronic documents must be produced intact and metadata cannot be altered or removed, except for the redaction of privileged or confidential information. Inadvertent production of metadata occurs when a document containing metadata is transmitted without the sender removing the metadata. This can occur when electronically sending documents such as briefs and discovery responses. The inadvertent production of metadata is an ethical issue for sending and receiving attorneys.

The Sending Attorney's Responsibilities

New Jersey Rule of Professional Conduct ("RPC") 1.6 prohibits lawyers from "reveal[ing] information relating to representation of a client" and New Jersey attorneys must take reasonable affirmative steps to prevent against possible inadvertent disclosure. While the New Jersey Advisory Committee on Professional Ethics has not addressed the issue of metadata and RPC 1.6 does not speak to a lawyer's duty concerning transmission of electronic documents, attorneys likely have an ethical responsibility under the RPCs to prevent the transmission of confidential client communications when sending electronic documents to anyone outside the attorney-client relationship. Attorneys must take affirmative steps to prevent sending this information.

An attorney who inadvertently transmits metadata containing confidential information without first obtaining the client's consent has likely breached his duty under RPC 1.6. Like the New Jersey rule, ABA Model Rule of Professional Conduct

1.6 states that an attorney “shall not reveal information relating to the representation of a client unless the client gives informed consent.” In Opinion 341, the D.C. Bar stated that attorneys must take reasonable steps to maintain the confidentiality of documents in their possession, including avoiding providing electronic documents that inadvertently contain metadata that is either a confidence or a secret. This mirrors opinions from Alabama, Florida, Maryland, and New York holding that an attorney has an ethical obligation to exercise reasonable care to safeguard the confidentiality of all attorney-client communications when transmitting electronic documents and not disclose protected information.

There are several ways to prevent the transmission of metadata. Certain types of electronic files, like those in Portable Document Format (“PDF”), contain less metadata than word processing documents. Word processing documents can be converted to or scanned into a PDF, affording senders a simple method to prevent the transmission of certain information or reduce the amount of metadata that is transmitted. Another easy method of preventing metadata transmission is to mail or fax a copy of the document. A foolproof way to ensure the removal of metadata is to use “scrubbing” software to screen documents and remove embedded information from them before they are electronically sent. Scrubbing removes a document’s metadata and produces a “clean” copy that can be sent to adversaries.

Upon learning that an electronic document sent to an adversary unknowingly contains metadata, an attorney should notify the adversary that any metadata was inadvertently produced and instruct the adversary not to review it.

Receiving Attorney’s Responsibilities

The ABA and some states have issued ethics opinions addressing attorneys’ use of inadvertently transmitted metadata. The ABA’s Formal Opinion 06-442 examined whether and to what extent receiving attorneys can review and use metadata and concluded that “the Model Rules of Professional Conduct do not contain any specific prohibition against a lawyer’s reviewing

and using embedded information in electronic documents. . . .” The ABA noted that the most closely applicable rule was Model Rule 4.4(b), which governs a lawyer’s receipt of inadvertently sent information, but that Rule does not address the propriety of a lawyer’s review of inadvertently disclosed information and provides only that “[a] lawyer who receives a document relating to the representation of the lawyer’s client and who knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.” Comment 3 to that Rule notes that the decision to utilize inadvertently disclosed information rests solely with the receiving lawyer. A lawyer receiving metadata need not notify his adversary unless he knows or reasonably should know that it was produced inadvertently, and he is not prohibited from reviewing and using any inadvertently transmitted data.

In Ethics Opinion 2007-09, the Maryland Bar Association Committee on Ethics followed the ABA’s approach. Other states have taken different positions. New York State Bar Opinion 749 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 [Lawyer’s Code of Professional Responsibility].” Similarly, in Ethics Opinion RO-2007-02, the Alabama Office of General Counsel concluded that “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.” Likewise, in Opinion 06-2, the Florida Bar determined that an attorney who obtains information from metadata that he knows or should know was not intended for him must notify the sending attorney.

Similarly, in Ethics Opinion 341, the D.C. Bar prohibited receiving attorneys from reviewing inadvertently transmitted metadata, but only where they have actual knowledge of the inadvertence. The D.C. Bar noted that an attorney who is unsure whether information was produced inadvertently should contact the sending attorney, though the receiving attorney is under no ethical obligation to do so. Importantly,

Opinion 341 does not prohibit receiving attorneys from reviewing and using information contained in metadata unless they have actual knowledge that the information was inadvertently sent.

Additionally, the D.C. Bar’s Opinion 341 requires “even in the context of discovery or other judicial process, if a receiving lawyer has actual knowledge that metadata containing protected information was inadvertently sent by the sending lawyer, the receiving lawyer . . . should advise the sending lawyer and determine whether such protected information was disclosed inadvertently.” Upon confirming that the protected information was unintentionally transmitted, the receiving attorney should then follow the sending attorney’s directives regarding the disposition of the document.

Responsibilities of New Jersey Attorneys

The New Jersey Committee has not addressed the issue of metadata, but it is likely that RPC 1.6 imposes an obligation on attorneys to take reasonable measures to prevent the inadvertent disclosure of metadata. It is less clear, however, what the obligations of receiving attorneys are. RPC 4.4(b) requires that “a lawyer who receives a document and has reasonable cause to believe that the document was inadvertently sent shall not read the document or, if he or she has begun to do so, shall stop reading the document, promptly notify the sender and return the document to the sender.” This rule appears to prohibit a receiving attorney from mining or using inadvertently transmitted metadata. Given the position that the committee has taken on this issue in the past with regard to hard copy documents, attorneys will likely be prohibited from reviewing metadata inadvertently sent with electronic documents. In the interim, attorneys faced with inadvertent disclosure of metadata must take into account the particular factual circumstances and be guided by the opinions issued by the ABA and the states that have addressed this question when deciding whether to review or use the information. At the same time, attorneys must take steps to prevent the transmission of protected information embedded in electronic files. ■