Wisconsin Formal Ethics Opinion EF-12-01: The Transmission and Receipt of Electronic Documents Containing Metadata

Revised April 27, 2018

Synopsis:

A lawyer who processes and transmits electronic documents containing information relating to the representation of clients to third parties must act competently to prevent the disclosure of significant information in the form of metadata contained in such documents.

A lawyer who receives an electronic document is not prohibited by the Rules from searching for metadata contained in such a document. However, a lawyer who chooses to review such a document for metadata and discovers information of material significance must normally assume such information was inadvertently disclosed and comply with SCR 20:4.4(b) or (c).

A lawyer who reviews an electronic document for metadata and discovers information that the lawyer knows or reasonably should know is protected by the lawyer-client privilege or the work product rule that has been disclosed inadvertently, must comply with SCR 20:4.4(c). Paragraph (c) requires the lawyer to immediately terminate review or use of the document or electronically stored information, promptly notify the person or the person's lawyer if communication with the person is prohibited by SCR 20:4.2 of the inadvertent disclosure, and abide by that person's or lawyer's instructions with respect to disposition of the document or electronically stored information until obtaining a definitive ruling on the proper disposition from a court with appropriate jurisdiction. If the lawyer does not know or cannot reasonably know that the inadvertently disclosed information is protected by the lawyer-client privilege or the work product rule, the lawyer is required by SCR 20:4.4(b)to promptly notify the sender.

Lawyers are not required to routinely search electronic documents for metadata.

Introduction

Metadata is embedded information contained in electronic documents. This information describes the document's history, tracking and management. By searching (i.e. "mining") for this data, it may be possible for a user to identify changes that were made to the document during its preparation and revision, comments made by the individuals that prepared or reviewed the document, and other information embedded within the document.

There are different types of metadata, different ways of creating it, and different ways of accessing it. For example, many word processing programs allow users to track changes made in a document. Tracking these changes allows users to identify what was added and deleted. These changes may be readily visible or hidden. However, even if the changes are hidden, other users can often locate them by simply clicking on a software icon contained in the program. Additionally, many programs such as Microsoft Word allow users to make comments on a document. Like track-changes, these comments may be visible or hidden. However, it may be possible for users to locate hidden comments by simply moving the cursor over their location or by changing the settings within the word document program itself. Metadata can also be accessed by the use of certain software.

While much of the metadata compiled in the creation of an electronic document may be of little importance, such as changes correcting simple spelling or grammatical errors, some of the information may have the potential to be damaging if it is shared with opposing counsel. Including such metadata in an electronic document shared with opposing counsel could result in the disclosure of confidential information, attorney work product or lawyer-client communications. A lawyer can avoid many of these consequences by being familiar with the types of metadata contained within an electronic document and by taking steps to protect or remove (i.e. "scrub") the information whenever it is necessary.

In this opinion, The State Bar's Standing Committee on Professional Ethics (the "Committee") discusses the duties arising under Wisconsin's Rules of Professional Conduct for Attorneys (the "Rules") associated with the transmission and receipt of documents containing metadata. It is important to note first that the obligations arising under the disciplinary rules discussed in this opinion do not take precedence over the discovery rules, either in state or federal court. Discovery of electronic material raises issues that extend beyond the scope of this opinion: this opinion discusses obligations of lawyers outside the context of formal discovery.

A. Ethical Obligations of the Transmitting Lawyer

1. The Duty of Competence

SCR 20:1.1 requires a lawyer to perform legal services competently.[1] ABA Comment [8], which follows SCR 20:1.1, recognizes that technology is an integral part of contemporary law practice and explicitly reminds lawyers that the duty to remain competent includes keeping up with technology.

> [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Moreover, ABA Comment [5], which follows SCR 20:1.1, recognizes that competency also requires the "use of methods and procedures meeting the standards of competent practitioners."

Lawyers who process and transmit electronic documents in their representation of clients are required by SCR 20:1.1 to stay reasonably informed about the types of metadata that are included in the electronic documents they generate and how to remove the metadata when necessary.[2] As technology evolves, the means of accessing and removing metadata will likely expand.[3]

The duty of competence applies to a lawyer's obligation to safeguard against the disclosure of protected information contained within electronic documents.

---

[1] SCR 20:1.1 Competence states:
"A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."

[2] "Competence requires that lawyers who use electronic documents understand that metadata is created in the generation of electronic documents, that transmission of electronic documents will include transmission of metadata, that recipients of the documents can access metadata, and that actions can be taken to prevent or minimize the transmission of metadata." Minnesota Lawyers Professional Responsibility Board, Opinion 22 (2010).

[3] *Id.*

2. The Duty of Confidentiality

The duty to protect information relating to the representation of the client is one of the most significant obligations imposed on the lawyer. SCR 20:1.6(a) prohibits a lawyer from revealing information relating to the representation of a client unless that client gives informed consent, unless the disclosure is impliedly authorized in order to carry out the representation, or unless the exceptions stated in paragraphs (b) and (c) apply.[4]

SCR 20:1.6(d), which became effective January 1, 2017, requires that a lawyer "make reasonable efforts to prevent inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Lawyers are not required, however, to guarantee that a breach of confidentiality cannot occur. ABA Comment [18], which follows SCR 20:1.6, emphasizes that unauthorized access to or the inadvertent or unauthorized disclosure of information relating to the representation of a client does not constitute a violation of the rule "if the lawyer has made reasonable efforts to prevent the access or disclosure."[5] The comment identifies a number of factors to be considered

---

[4] SCR 20:1.6 Confidentiality states:

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in pars. (b) and (c).

(b) A lawyer shall reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary to prevent the client from committing a criminal or fraudulent act that the lawyer reasonably believes is likely to result in death or substantial bodily harm or in substantial injury to the financial interest or property of another.

(c) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably likely death or substantial bodily harm;

(2) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(3) to secure legal advice about the lawyer's conduct under these rules;

(4) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;

(5) to comply with other law or a court order; or

(6) to detect and resolve conflicts of interest, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

(d) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

[5] ABA Comment [18] states:

> Acting Competently to Preserve Confidentiality
>
> [18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and 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. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and

in determining the reasonableness of the lawyer's efforts. These factors "include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)." Consequently, the determination of what constitutes reasonable precautions to avoid disclosure of confidential information may vary according to the circumstances of each case.

At least nineteen other states have ethics opinions considering the ethical obligations of lawyers with respect to metadata,[6] and there is near unanimous agreement that lawyers who send electronic documents are ethically required to take reasonable care to avoid the disclosure of protected information contained within metadata.[7]

As noted above, some metadata is of little or no importance, and lawyers do not violate their ethical duties by failing to remove such metadata. Also, in some situations, lawyers may intentionally wish to provide documents containing metadata, or may be required by law to refrain from scrubbing documents for metadata. Lawyers must, however, be cognizant of when the metadata contained within a document is of such importance that the lawyer is ethically obligated to prevent disclosure. Moreover, unless lawyers obtain a reasonable understanding of the risks inherent in processing, sending and receiving electronic documents, and the reasonable steps necessary to prevent any unintended disclosure, they risk violating their duty of confidentiality to clients. To fulfill their duty of confidentiality, lawyers must either familiarize themselves sufficiently with the technological means to detect metadata and remove it, when necessary, or to obtain the assistance of someone possessing such knowledge. Due to the rapidly changing nature of technology, it is beyond the scope of this opinion to detail specific methods for removing metadata from electronic documents.

> federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

Similarly, ABA Comment [19], which follows SCR 20:1.6, requires a lawyer, when transmitting a communication that includes information relating to the representation of the client, to take reasonable precautions to prevent the information from coming into the hands of unintended recipients. ABA Comment [19] states:

> [19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

[6] American Bar Association Law Practice Division, Metadata Ethics Opinions Around the U.S., https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html . This chart does not include Texas State Bar Association Professional Ethics Committee Opinion 665 (12/2016) and Missouri Bar Informal Advisory Opinion 2014-02.

[7] *Id.* See, e.g., Texas State Bar Association Professional Ethics Committee Opinion 665 (12/2016); Washington State Bar Association Rules of Professional Conduct Committee Advisory Opinion 2216 (2012); Minnesota Lawyers Professional Responsibility Board Opinion 22 (2010); North Carolina State Bar Ethics Committee, 2009 Formal Ethics Opinion 1.

B. Ethical Obligations of the Receiving Lawyer

Three distinct questions arise related to a receiving lawyer's obligations regarding metadata. First, may the receiving lawyer ethically mine for and review metadata? Second, if a receiving lawyer may mine for metadata, what must the lawyer do if the metadata contains material information? Third, is the receiving lawyer required by the duty of competence to actively search documents for metadata?

1. May a receiving lawyer ethically mine for metadata?

While the majority of jurisdictions agree that lawyers processing and transmitting electronic documents have a duty to use reasonable care to guard against the disclosure of metadata that may contain confidential information, there is a pronounced split regarding whether it is permissible for lawyers to mine for and use metadata received from opponents or third parties.

On the one hand, the State Bar of Arizona Committee on the Rules of Professional Conduct concluded that "a lawyer who receives an electronic communication may not examine it for the purpose of discovering the metadata embedded in it."[8] This conclusion was shared by the bar association ethics committees of Alabama, Maine, New York, and New Hampshire.[9] The ethical foundation for these opinions rests on the belief that attorneys who search for metadata are unjustifiably infringing on the opposing counsel's confidential relationship with his or her client, which is conduct these jurisdictions believe to be dishonest or deceitful, and thus in violation of Model Rule 8.4(c). Additionally, some jurisdictions, such as Alabama, also believe that attorneys who search for metadata are engaging in conduct that violates their version of ABA Model Rule 8.4(d), which prohibits attorneys from engaging in conduct that "is prejudicial to the administration of justice."[10]

On the other hand, the American Bar Association Committee on Ethics and Professional Responsibility concluded that receiving lawyers may review information contained in metadata in certain circumstances.[11] The opinion concluded that the Model Rules of Professional Conduct do not prohibit attorneys from mining for and using metadata they received from opposing counsel. This conclusion was shared by the bar associations in Colorado and Vermont. The Colorado Bar Association Ethics Committee

---

[8] State Bar of Arizona Committee on the Rules of Professional Conduct, Ethics Op. 07-03 (2007).

[9] *See,* Alabama State Bar Office of General Counsel Formal Ethics Op. 2007-02 (2007) (the receiving lawyer has "an ethical obligation to refrain from mining an electronic document); State of Maine Board of Overseers of the Bar Professional Ethics Commission Op. 196 (2008) ("an attorney may not ethically take steps to uncover metadata, embedded in an electronic document sent by counsel for another party, in an effort to detect information that is legally confidential and is or should be reasonably known not to have been intentionally communicated"); New York Committee on Professional Ethics Op. 749 (2001) ("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"); New Hampshire Bar Association Ethics Committee Advisory Op. 2008-2009/4 (receiving lawyers must "refrain from reviewing metadata.")

[10] *See*, Alabama State Bar Office of General Counsel, Formal Ethics Op. 2007-02 ("[t]he 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.")

[11] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-442 (2006).

concluded that "a Receiving Lawyer generally may ethically search for and review metadata embedded in an electronic document that the Receiving Lawyer receives from opposing counsel or other third party."[12] The Vermont Bar Association Professional Responsibility Section found "nothing to compel the conclusion that a lawyer who receives an electronic file from opposing counsel would be ethically prohibited from reviewing that file using any available tool to expose the file's content, including metadata."[13] The Texas State Bar Professional Ethics Committee concluded more broadly that the ethics rules "do not prohibit a lawyer from searching for, extracting, or using metadata" embedded in documents received from opponents.[14]

Other jurisdictions adopted variations of the Arizona and ABA views. For example, both Oregon Formal Ethics Opinion 2011-187, which was revised in 2015, and Washington Informal Ethics Opinion 2216[15] concluded that while lawyers may review readily accessible metadata, they may not use sophisticated forensic software to extract metadata from a scrubbed document. The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility concluded that the ethical obligations of a receiving attorney would be made on a case-by-case basis.[16] The Pennsylvania opinion stated that a receiving attorney "(a) must determine whether he or she may use the data received as a matter of substantive law; (b) must consider the potential effect on the client's matter should the lawyer do so; and, (c) should advise and consult with the client about the appropriate course of action under the circumstances."[17] Similarly, Minnesota Lawyers Professional Responsibility Board did not establish a clear rule regarding the mining of metadata, but instead concluded that "[w]hether and when a lawyer may be advised to look or not to look for metadata is a fact specific question beyond the scope of this Opinion."[18] The District of Columbia Bar Ethics Committee concluded, however, that Rule 8.4 is implicated only when the receiving lawyer has actual prior knowledge that the metadata was inadvertently provided: "we believe that mere uncertainty by the receiving lawyer as to the inadvertence of the sender does not trigger an ethical obligation by the receiving lawyer to refrain from reviewing that metadata."[19]

Having considered the approaches and rationales of the various jurisdictions, the Committee does not believe that the Rules prohibit Wisconsin lawyers from searching for metadata in documents received from opposing counsel or third parties. This conclusion is supported by the following considerations.

First, the Committee agrees with the ABA and does not believe that a receiving lawyer is engaging in deceitful or dishonest behavior when searching for metadata contained within electronic documents. Much of the metadata contained within an electronic document can be revealed by simply clicking on a software icon or by moving a cursor over a document. Even when more elaborate methods are used to

[12] Colorado Bar Association Ethics Committee, Formal Ethics Op. 119 (2008).

[13] Vermont Bar Association Professional Responsibility Section, Advisory Ethics Op. 2009-1 (2009).

[14] Texas State Bar Professional Ethics Committee, Op. 665 (2016).

[15] Oregon Formal Ethics Opinion 2011-187 (2011, revised 2015); Washington Informal Ethics Opinion 2216 (2012).

[16] Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility, Formal Ethics Op. 2009-100.

[17] *Id.*

[18] Minnesota Lawyers Professional Responsibility Board, Ethics Op. 22 (2010).

[19] District of Columbia Bar Ethics Committee, Ethics Op. 341 (2007).

mine for metadata, there is nothing inherently deceitful or dishonest or unfair about such tactics. Therefore, searching documents received from opposing parties does not violate SCR 20:8.4(c)[20] or SCR 20:8.4(g).[21] Second, unlike states such as Alabama, Wisconsin does not have an equivalent of ABA Model Rule 8.4(d), which prohibits attorneys from engaging "in conduct that is prejudicial to the administration of justice," and therefore such a Rule cannot be invoked to prohibit lawyers from searching for metadata.[22] Third, an absolute bar on reviewing metadata ignores the fact that lawyers may, in certain circumstances, be compelled by their duty of competent representation to closely examine documents received from opponents or third parties. Fourth, SCR 20:4.4(c) specifically protects metadata that contains information subject to the lawyer-client privilege and the work product rule. Therefore, it is the opinion of the Committee that Wisconsin's Rules do not prohibit lawyers from searching for and reviewing metadata included in an electronic document. A lawyer who searches an electronic document for metadata does not violate Wisconsin's Rules.

Finally, given the split among jurisdictions, Wisconsin attorneys who appear in other jurisdictions should be aware of the rules regarding metadata in those jurisdictions.

2. What are the receiving lawyer's obligations on discovering metadata that appears to contain material information?

Much of the metadata embedded in an electronic document is of little importance. This information, such as changes in punctuation and grammar, is not material to the representation. If a lawyer discovers metadata that is not material to the representation, the Committee does not believe that SCR 20:4.4(b) and (c) apply, and the lawyer has no obligations arising under those paragraphs. However, when metadata contains material information, the receiving lawyer is bound by the obligations contained in SCR 20:4.4(b) and (c).

SCR 20:4.4(b) and (c) govern the ethical obligations of a lawyer who receives electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the electronically stored information was inadvertently sent or disclosed. "Electronically stored information" is defined in ABA Comment [2] to specifically include metadata.[23] ABA Comment [2] also defines "inadvertently sent" to include metadata that is "accidentally included with information that was

[20] The Committee rejected the notion that that searching for metadata is potentially dishonest because the only metadata worth searching for consists of another's property whose value may be diminished, destroyed or misappropriated by the very act of discovery.

[21] The Committee also concluded that mining for metadata does not violate the Attorney's Oath, SCR 40.15, which mandates that attorneys use such means only that are consistent with honor. The Committee rejected the notion that mining for metadata is unfair because, unlike formal discovery, the adversary is not given fair warning of the information sought and an opportunity to protect its confidentiality if appropriate.

[22] The closest analogy to MR 8.4(d) in Wisconsin's Rules is SCR 40:15 (the Attorney's Oath), which, pursuant to SCR 20:8.4(g), is misconduct to violate. The majority of Committee, however, does not believe that any of the provisions of SCR 40.15 prohibit a lawyer from searching for metadata.

[23] ABA Comment [2], which follows SCR 20:4.4 states in part:

> . . . For purposes of this Rule, "document or electronically stored information" includes, in addition to paper documents, email or other forms of electronically stored information, including embedded data (commonly referred to as "metadata"), that is subject to being read or put into readable form. . . .

intentionally transmitted."[24] Paragraph (c), which became effective on January 1, 2017, specifically applies to metadata containing information that is protected by the attorney-client privilege or the work product rule. Paragraph (b) applies to metadata containing material information other than information protected by the attorney-client privilege or the work product rule.

SCR 20:4.4(b) states:

> (b) A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender.

SCR 20:4.4, unlike its Model Rule counterpart, contains paragraph (c), which specifically applies to information protected by the lawyer-client privilege and the work product rule.

> (c) A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information contains information protected by the lawyer-client privilege or the work product rule and has been disclosed to the lawyer inadvertently shall:
>
> (1) immediately terminate review or use of the document or electronically stored information;
>
> (2) promptly notify the person or the person's lawyer if communication with the person is prohibited by SCR 20:4.2 of the inadvertent disclosure; and
>
> (3) abide by that person's or lawyer's instructions with respect to disposition of the document or electronically stored information until obtaining a definitive ruling on the proper disposition from a court with appropriate jurisdiction.

The duties imposed by paragraph (c) reflect the importance of the lawyer-client privilege and the work product rule, and recognize that protecting the lawyer-client privilege promotes the functioning of the justice system. These duties are consistent with *Harold Sampson Children's Trust v. The Linda Gale Sampson 1979 Trust,* 2004 WI 57, 271 Wis. 2d 610, 679 N.W.2d 794 (2004), which concluded that a lawyer, without the consent or knowledge of a client, cannot waive the lawyer-client privilege by voluntarily producing privileged documents, which the lawyer does not recognize as privileged, to an opposing attorney in response to a discovery request. The court held that only the client can waive the lawyer-client privilege under Wis. Stat. § 905.11 (2015-2016) regarding attorney-client privileged documents. The duties imposed by paragraph (c) are also consistent with Wis. Stat. § 804.01(7) (2015-2016), which governs recovering information inadvertently disclosed in discovery.

Moreover, the duties imposed by paragraph (c) reflect the concern that SCR 20:4.4, prior to its amendment adding paragraph (c), provided no guidance for the receiving lawyer. Under paragraph (b), the lawyer's sole obligation upon receiving any representation-related document that the lawyer knew

[24] ABA Comment [2] state in part:

> "…A document or electronically stored information is inadvertently sent when it is accidentally transmitted, such as when an email or letter is misaddressed or a document or electronically stored information is accidentally included with information that was intentionally transmitted…"

or reasonably should have known was inadvertently sent was to "promptly notify the sender."[25] The addition of paragraph (c) distinguishes between the types of information inadvertently disclosed and imposes the additional obligations beyond prompt notification when the receiving lawyer knows or reasonably should know that the information is protected by the lawyer-client privilege or the work product rule.

Absent circumstances indicating otherwise, a receiving lawyer should normally assume that any metadata of material significance was inadvertently transmitted. It is reasonable to expect that a sending lawyer will attempt to competently represent his or her client. It is also reasonable to expect that a sending lawyer will attempt to protect the information relating to the representation of his client. Accordingly, it is reasonable to assume that a sending lawyer would not intentionally transmit to opposing counsel metadata containing confidential information of material significance.

It is not possible to enumerate every category of information that may be of material significance, but lawyers should normally assume that any information that is relevant and the disclosure of which is potentially detrimental to the sending party to fall within this category. For example, a lawyer should normally consider information about legal strategies, settlement parameters, previously undisclosed relevant facts, and any information which appears to be privileged to be information of "material significance" and consequently inadvertently disclosed.

Finally, the duty of notification arising under SCR 20:4.4(b) and (c) supersede the duty of confidentiality arising under SCR 20:1.6. Thus, a lawyer discovering metadata of material significance must notify the sender even if the lawyer's client instructs the lawyer not to provide such notification.

3. Is a receiving lawyer required by the duty of competence to actively search documents for metadata?

As stated above, Wisconsin's Rules of Professional Conduct require attorneys to take reasonable steps to prevent the inadvertent disclosure of confidential information contained within electronic documents. Additionally, Wisconsin's Rules of Professional Conduct do not prohibit attorneys from searching for metadata contained within electronic documents. Thus, the question arises whether lawyers are required by their duty of competence to actively search documents for metadata. The Committee does not believe that any such general duty exists because there is no reasonable basis to conclude that any specific document would contain significant metadata.

Under SCR 20:1.1, it is reasonable to expect that a sending attorney will attempt to competently represent his or her client. Under SCR 20:1.6, it is also reasonable to expect that a sending attorney will attempt to protect information relating to the representation of the client from inadvertent disclosure. Accordingly, a receiving attorney may normally reasonably believe that any metadata of material significance was removed from an electronic document prior to its transmission. Thus, there would be no reasonable basis for an attorney to conclude that any specific document would contain significant metadata. Since there is no reasonable basis for concluding that any electronic document contains

[25] Paragraph (b) did not require the receiving lawyer to return the document or preserve it. It did not specify whether the lawyer was permitted to read the document if the lawyer already knew that the document was sent in error, or whether the lawyer was required to stop reading upon realizing the error. Nor did paragraph (b) draw any distinction based on whether the document or information looked privileged. Whatever the lawyer was required or permitted to do was beyond the scope of the Rule.

significant metadata, SCR 20:1.1 does not require Wisconsin attorneys to actively search documents for metadata.

Further, as stated above, lawyers normally should assume that metadata of material significance was inadvertently sent and therefore, should comply with SCR 20:4.4(b) or (c). This supports the conclusion that lawyers do not have an affirmative duty arising under the Rules to routinely search documents for metadata. The Committee notes however, that specific circumstances may warrant that a lawyer search a specific document for metadata.

Conclusion

Wisconsin lawyers should be aware of the ethical responsibilities associated with the transmission and receipt of electronic documents containing metadata. Lawyers who send electronic materials are ethically required to take reasonable care to avoid the disclosure of information protected by the duty of confidentiality that is contained within metadata. Additionally, it is permissible for Wisconsin attorneys to search for metadata contained within electronic documents. However, when an electronic document contains material metadata, and the lawyer knows or reasonably should know that the metadata was inadvertently sent, the lawyer must comply with SCR 20:4.4(b) or (c). Furthermore, it should be noted that the ability to mine for and review metadata contained within an electronic document does not create an ethical obligation for Wisconsin attorneys to actively search for metadata contained within electronic documents.