SUPREME COURT OF ARIZONA

ATTORNEY ETHICS ADVISORY COMMITTEE

Ethics Opinion File No. EO-20-0008

The Attorney Ethics Advisory Committee was created in accordance with Rule 42.1.

A lawyer who authors and sends an electronic document to someone other than the client on whose behalf the document was drafted, or other privileged persons, is responsible, under ER 1.6, for first scrubbing the document of confidential metadata that may be contained within the electronic file using standard software applications for doing so.

A lawyer who receives an electronic document or other type of electronic file from another lawyer may ethically use the software applications within which the file was created and saved to retrieve and review embedded metadata unless the lawyer knows or reasonably should know that the metadata was included inadvertently—in which case the receiving lawyer should follow the process in ER 4.4(b). Metadata that contains material information that the lawyer knows or reasonably should know is confidential or privileged should be assumed to be inadvertently disclosed. "Mining" for metadata, meaning searching for metadata using software applications that are designed to retrieve metadata despite a sending lawyer's reasonable efforts to scrub it, violates ER 4.4(a). This opinion approves in part and disapproves in part State Bar of Arizona Opinion 07-03.

A lawyer may not, without the prior informed consent of the recipient, ethically embed in an email to potential, current, or future clients, or other lawyers, hidden email-tracking software, also known as a web beacon, pixel tag, clear GIF or invisible GIF. Use of such a device violates ER 4.4.

ISSUES PRESENTED

1. If a lawyer sends an electronic communication, what ethical duty does the lawyer have to prevent the disclosure, through metadata embedded therein, of confidential or privileged information?

2. May a lawyer who receives an electronic communication examine it for the purpose of discovering the contents of the metadata that may be embedded within it?

3. May a lawyer embed hidden software in an email to another lawyer that tracks information about the handling and viewing of the email?

RELEVANT ETHICS OPINIONS

State Bar of Arizona, Rules of Professional Conduct committee, Opinion No. 07-03

ABA Formal Op. 06-442

APPLICABLE ARIZONA RULES OF PROFESSIONAL CONDUCT

ER 1.0 Terminology

***

(f) "Knowingly," "known," or "knows" denotes actual knowledge of the fact in question. A person's knowledge may be inferred from circumstances.

***

(i) "Reasonably should know" when used in reference to a lawyer denotes that a lawyer of reasonable prudence and competence would ascertain the matter in question.

ER 1.1. Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

***

Comment

***

Maintaining Competence

[6] 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.

***

ER 1.6. Confidentiality of Information

(a) 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 or required by paragraphs (b), (c) or (d), or ER 3.3(a)(3).

***

Comment

***

Acting Competently to Preserve Confidentiality

[22] Paragraph (e) 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 ERs 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 (e) if the lawyer has made reasonable efforts to prevent the access or disclosure. …

ER 4.4. Respect for Rights of Others

(a) In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden any other person, or use methods of obtaining evidence that violate the legal rights of such a person.

(b) A lawyer who receives a document or electronically stored information and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender and preserve the status quo for a reasonable period of time in order to permit the sender to take protective measures.

Comment

[1] Responsibility to a client requires a lawyer to subordinate the interests of others to those of the client, but that responsibility does not imply that a lawyer may disregard the rights of others. It is impracticable to catalogue all such rights, but they include legal restrictions on methods of obtaining evidence from others and unwarranted intrusions into privileged relationships, such as the client-lawyer relationship.

[3] … A receiving lawyer who discovers metadata embedded within a document or electronically stored communication and who knows or reasonably should know that the metadata reveals confidential or privileged information has a duty to comply with the procedures set forth in ER 4.4(b).

ER 8.4. Misconduct

It is professional misconduct for a lawyer to:
***
(c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation;

***

OPINION

Metadata

Electronic documents and other electronic files contain "metadata" – information about the file, such as when and by whom it was created, when and how and by whom it was subsequently edited and modified, and even embedded "comments." SBA Opinion 07-03 concludes that a lawyer sending an electronic document to anyone—other than the client, other lawyers and staff within the lawyer's firm, or other privileged persons—must take reasonable measures to "scrub" the document of such confidential information, except to the extent prohibited by a rule, order, or procedure of a court or other applicable provision of law.

This is consistent with the ethics opinions of all other jurisdictions that have addressed the issue and the Committee agrees with this conclusion. The burden to ensure that confidential information

is protected rests in the first instance on the shoulders of the sending lawyer, and it is by no means a heavy burden. "Scrubbing" software is commonly available. It is even included within the programs—Microsoft Word and Adobe Pro, for example—that lawyers most often use to create most of the electronic files they create and share. Understanding how to run these simple processes—or relying on staff that are proficient at running them—is part of a lawyer's duty of competence under ER 1.1. Ariz. R. Sup. Ct., Rule 42, ER 1.1, cmt. ¶ 6 (duty to "keep abreast of changes in the law and its practice**,** including the benefits and risks associated with relevant technology").

The degree of electronic scrubbing that is required will depend on the circumstances. Some information may be so innocuous that a lawyer is, under the circumstances, justified in concluding that its disclosure is impliedly authorized by the client – for example, information about when and by whom the document was created and modified when this is already generally known to the receiving party or is simply immaterial. More sensitive metadata, which will typically include things like the history of substantive edits and embedded comments made or inserted by the lawyer or the client—particularly any privileged communications between the lawyer and client—should be removed before the lawyer shares the file with a non-privileged person.

This of course does not in any way limit the professional obligation of the lawyer to provide a "redlined" document to the lawyers for other parties that show changes made to a draft joint document under negotiation (whether a motion, stipulation, contract, etc.) (*see* Ariz. R. Sup. Ct., Rule 41, *Creed of Professionalism* § B(12)), nor does it limit the obligation to provide files in their native format, with intact metadata, when required by discovery and disclosure rules or other applicable law.

The SBA Opinion, however, goes on to conclude that a lawyer who *receives* an electronic document or other file may not deliberately access and review any metadata embedded in it, but rather must treat the metadata as "inadvertently sent" within the meaning of ER 4.4(b)—even when the electronic document itself was not inadvertently sent—unless review is otherwise allowed by a rule, order, or procedure of a court or other applicable provision of law. There are a few opinions from other jurisdictions that take this same general approach. *See* North Carolina Bar 2009 Formal Ethics Opinion 1 (January 15, 2010); Maine board of Overseers of the Bar Professional Ethics Commission Opinion #196, *Transmission, Retrieval and Use of Metadata Embedded in Documents* (October 21, 2008); New Hampshire Bar Association Ethics Committee Advisory Opinion #2008-09/04, *Disclosure, Review, and Use of Metadata in Electronic Materials* (May 15, 2009); *Professional Ethics of the Florida Bar Opinion 06-2* (September 15, 2006); New York State Bar Association Committee on Professional Ethics Opinion Number 749 (December 14, 2001).

But, as noted by a Colorado ethics opinion, these opinions "appear to be based on an implied premise that searching for metadata is surreptitious or otherwise involves procedures that are difficult or complicated. They also seem to assume that metadata generally contain Confidential Information and that any metadata transmitted to a third party must, therefore, have been transmitted inadvertently." Colorado Formal Opinion 119, *Disclosure, Review, and Use of Metadata* (May 17, 2008). The Committee agrees that these assumptions are generally unwarranted and therefore rejects the blanket prohibition in the SBA Opinion and instead

concludes that the receiving lawyer does not act unethically by reviewing metadata that is readily viewable within the file's native software application or normal operating systems unless the lawyer knows or reasonably should know that the document itself was inadvertently sent or was sent with the metadata inadvertently included.

Though "mere uncertainty" does not rise to the level of actual or constructive knowledge (The District of Columbia Bar Association Ethics Opinion 341 (September 2007)), inadvertence may be inferred from the nature of the metadata. Specifically, metadata that appears to be material confidential information or that reveals privileged communications or work product should be assumed by the receiving lawyer to have been inadvertently provided by the sending lawyer, and the receiving lawyer should follow the ER 4.4(b) process. This is consistent with the comment to Arizona's version of ER 4.4 (see cmt. ¶ 3), and with the approach of most other jurisdictions that have addressed the issue. In addition to the Colorado and D.C. opinions, *see* Wisconsin Formal Ethics Opinion EF-12-01, *The Transmission and Receipt of Electronic Documents Containing Metadata* (Rev. April 27, 2018); Texas State Bar Association Professional Ethics Committee Opinion 665 (December 2016); Pennsylvania Bar Association Committee On Legal Ethics and Professional Responsibility, Formal Opinion 2009 – 100, *Ethical Obligations on the Transmission and Receipt of Metadata* (2009); Maryland State Bar Association Committee on Ethics Opinion 2007-09, *Ethics of Viewing and/or Using Metadata* (January 1, 2007).

The Committee also, however, agrees with the three jurisdictions that have distinguished between permissible viewing of readily discernable metadata and truly "mining" for metadata, and have found the latter to be ethically problematic.

> 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.

Mississippi Bar Ethics Opinion No. 259 (November 29, 2012). *See also* Oregon Formal Opinion No. 2011-187 (revised 2015); and Washington State Bar Association Advisory Opinion 2216 (2012). Using special software to discover metadata despite the sending lawyer's reasonable efforts to scrub it is analogous to taking a document out of another lawyer's briefcase when their back is turned. The briefcase owner may have a duty to ensure that the briefcase isn't standing open on opposing counsel's conference table with sensitive material at the top of its contents, but they shouldn't have to lock it.

Web Bugs

The Committee received an inquiry regarding whether it is ethical for a lawyer to embed a "web bug" in emails to other lawyers. As described in an opinion issued by the Illinois State Bar Association Professional Conduct Advisory Committee, a "web bug"—also called a web beacon,

pixel tag, clear GIF or invisible GIF[1]—is a piece of software, hidden with an email message, that "permit[s] the sender of an email message to secretly monitor the receipt and subsequent handling of the message, including any attachments":

> The specific technology, operation, and other features of such software appear to vary among vendors. Typically, however, tracking software inserts an invisible image or code into an email message that is automatically activated when the email is opened. Once activated, the software reports to the sender, without the knowledge of the recipient, detailed information regarding the recipient's use of the message. Depending on the vendor, the information reported back to the sender may include: when the email was opened; who opened the email; the type of device used to open the email; how long the email was open; whether and how long any attachments, or individual pages of an attachment, were opened; when and how often the email or any attachments, or individual pages of an attachment, were reopened; whether and what attachments were downloaded; whether and when the email or any attachments were forwarded; the email address of any subsequent recipient; and the general geographic location of the device that received the forwarded message or attachment. At the sender's option, tracking software can be used with or without notice to the recipient.

ISBA Professional Conduct Advisory Opinion No. 18-01 (January 2018). It is easy to imagine the various ways in which such information might provide the sending lawyer with significant insights into the receiving lawyer's work project, the lawyer's communications to and from their client, and how the lawyer and client evaluate the information in the email (and any documents attached) and hence the matter within which the email has been generated. Importantly, unlike with metadata-scrubbing software, there does not appear to be any readily available and consistently reliable devices or programs capable of detecting or blocking web bugs before they have transmitted data about the email recipient. Therefore, if a lawyer chooses to use a web bug, there is no realistic way for the receiving lawyer to protect themselves.

The Illinois ethics opinion, as well opinions issued in Pennsylvania, Alaska, and New York, conclude that the use of such software is ethically prohibited. *See* Pennsylvania Bar Association Legal Ethics and Professional Responsibility Committee Formal Opinion No. 2017-300 (2017); Alaska Bar Association Ethics Opinion No. 2016-1 (October 2016); New York State Bar Association Opinion 749 (December 2001). The Committee agrees with the reasoning and conclusions of these opinions. The use of such software constitutes an "unwarranted intrusion[] into … the client-lawyer relationship," which violates ER 4.4's prohibition on a lawyer's employment of "methods of obtaining evidence that violate the legal rights of such a person." Ariz. R. Sup. Ct., Rule 42, ER 4.4(a) and Comment ¶ 1. It also falls within ER 8.4's prohibition of

[1] This opinion does not encompass services such as Constant Contact or MailChimp that track emails but do so prominently displayed links and images that the email recipient can choose not to click.

“conduct involving dishonesty, fraud, deceit or misrepresentation. Ariz. R. Sup. Ct., Rule 42, ER 8.4(c).