

**ALASKA BAR ASSOCIATION
ETHICS OPINION NO. 2016-1**

**May a Lawyer Surreptitiously Track Emails and Other Documents
Sent to Opposing Counsel?**

Issue Presented: Is it ethically permissible for a lawyer to use a “web bug” or other tracking device to track the location and use of emails and documents sent to opposing counsel?

Conclusion: No. The use of a tracking device that provides information about the use of documents – aside from their receipt and having been “read” by opposing counsel – is a violation of Rule 8.4 and also potentially impermissibly infringes on the lawyer’s ability to preserve a client’s confidences as required by Rule 1.6.

Background: A member of the Alaska Bar recently received an email with a “web bug” from opposing counsel. A web bug is a technology tool that tracks certain information about the document to which it is attached. A common method of “web bugging” – used in e-mail newsletters to help track readers, for example – involves placing an image with a unique website address on an Internet server. The document at issue contains a link to this image. The image may be invisible or may be disguised as a part of the document (e.g., part of a footer). When the recipient opens the document, the recipient’s computer looks up the image and thereby sends certain information to the sending party.

One commercial provider of this web bug service advertises that users may track emails “invisibly” (i.e., without the recipient’s knowledge) and may also track, among other details:

- when the email was opened;
- how long the email was reviewed (including whether it was in the foreground or background while the user worked on other activities);
- how many times the email was opened;
- whether the recipient opened attachments to the email;
- how long the attachment (or a page of the attachment) was reviewed;
- whether and when the subject email or attachment was forwarded; and
- the rough geographical location of the recipient.¹

This provider and similar services give the sender options to alert the recipient that the email contains a web bug and is being tracked, but the sender also has the ability not to disclose this information – which indeed seems to be the main point of the product. If the sender elects not to notify the recipient that the email or document contains a web bug, some email systems or software programs (e.g., Adobe) may either reject the web bug or affirmatively notify the recipient of its existence. Not all email systems or software programs, however, will identify a

¹ See Live Sample Receipt of ReadNotify Email Tracking History, <http://www.readnotify.com/readnotify/show.asp/0015c797da9a070e0a72c9dd2769d956.html> (last visited August 29, 2016).

tracking device and notify the recipient. And, given the speed at which this technology is developing, it cannot be said with any assurance that detection programs will be consistently effective in discovering and reporting web bugs or other tracking devices.

Analysis: Rule 8.4(c) provides that “[i]t is professional misconduct for a lawyer to . . . engage in conduct involving dishonesty, fraud, deceit, or misrepresentation.” In earlier opinions, the Committee has offered some guidance as to the type of conduct that would run afoul of this rule. For example, a lawyer instructing a court reporter not to inform opposing counsel that the lawyer had requested transcription of a deposition would be unethical if the lawyer knew that opposing counsel expected to receive notice.²

A closer analog to the current situation arose in Opinion 2003-1, which withdrew earlier ethics opinions prohibiting the undisclosed recording of telephone conversations by a lawyer. In Opinion 2003-1, the Committee noted that in the 1970s there was a general assumption that anyone speaking with a lawyer would justifiably believe that the conversation was not being recorded.³ Given that assumption, a lawyer who recorded a conversation without giving appropriate notice or obtaining consent had engaged in misrepresentation or deceit.⁴ In Opinion 2003-1 the Committee noted that with the increasing prevalence of telephone recording devices this assumption no longer held true. Accordingly, there was no implied representation that lawyers would not record conversations with other participants and no basis for a *per se* finding of dishonesty, fraud, deceit, or misrepresentation if a recording was made without disclosure.⁵

The use of “web bugs” and other tracking devices is fundamentally different from the permissible recording of conversations by a lawyer. Unlike the telephone recording situation, the Committee believes that it is entirely reasonable for a lawyer to assume that emails, documents and other electronic communications received from an opposing lawyer will not be

² See Opinion 88-4 (applying DR1-102(A)(4), the precursor to Rule 8.4(c)).

³ See Opinion 2003-1, at 2 (discussing withdrawn opinion 78-1 and ABA Formal Opinion 337).

⁴ See *id.*

⁵ See *id.* at 3. (“In the absence any rule or statute specifically prohibiting lawyers from recording conversations without notice, we are confronted with the issue of whether a lawyer violates any Rule of Professional Conduct by reliably preserving information through recording, without notice to other parties to the conversation. The act of recording a conversation, standing alone, is not harmful to a party who has not been advised of or consented to the recording. An undisclosed recording might, however, be used in a manner that would be harmful to an individual. Examples include recording or preserving only portions of the conversation to distort its content, using a recording to embarrass the other party to the conversation or a third party, or improper disclosure of a client confidence contained in a recording. But any such misuse of a recorded statement can be addressed by application of the Rules without straining to interpret the Rules as creating a *per se* prohibition against undisclosed recording.”).

“bugged.” And, consistent with Opinion 88-4, the Committee likewise believes that it is unethical to use tracking devices on electronic communications.

Most importantly, a core difference from the recording of conversations is that discussions with opposing counsel are not privileged or confidential. Whether or not the conversation is recorded, the communication has been knowingly shared with opposing counsel. This is not true with a tracked electronic communication, especially when the tracking device is undisclosed. If the tracking device is performing as designed, a lawyer will have no idea that the sending lawyer is tracking the lawyer’s handling of the communication. The tracking device could enable the sending lawyer to learn how much time the receiving lawyer spent reviewing the communication – including even specific pages of documents – or how frequently the communication was viewed (a proxy for how important the receiving lawyer deemed it to be), whether and when it was forwarded either to the client or co-counsel or otherwise, the location of the recipients, and the details of the recipients’ review of the document.

As just one example, assume that a client informs her lawyer that she has moved to another state but does not want her whereabouts disclosed to anyone else for any number of reasons. Opposing counsel sends a bugged email to the client’s lawyer that includes an attached document for the client’s signature. When that email is forwarded to the client, the tracking device could improperly obtain and deliver to the sending lawyer confidential information about the client’s general location.⁶ Or, assume that the parties are in settlement negotiations and one lawyer sends a bugged email with a draft settlement agreement. Based on the report from the tracking device, the sending lawyer learns that the lawyer focused most of her time on the third page; the lawyer then forwarded the document to a city where the client lives; this recipient focused on the sixth page and then sent the document back to the lawyer; and the lawyer subsequently focused solely on the sixth page of the draft. This gives the sending lawyer access to attorney-client protected information and extraordinary insight as to which sections of a document the lawyer and her client found most important.

While the surreptitious use of tracking devices is especially troubling, even the disclosed use of a tracking device when communicating with opposing counsel is not permissible. Insofar as the tracking device allows the sending lawyer to intrude upon the attorney’s work product by tracking the attorney’s use of that document, it constitutes an unwarranted intrusion into the attorney-client relationship.⁷ Seeking to invade that relationship through the use of tracking

⁶ Cf. Idaho Bar. Op. 96 (1977) (concluding that disclosing a client’s location would be a violation of the lawyer’s duty to preserve the client’s confidences). The use of “delivery receipts” and “read receipts” through Outlook and similar email services does not intrude upon the attorney’s work product or track the use of a document, and therefore is not at issue here. Those types of receipts are functionally comparable to the receipt one may receive from the use of certified mail.

⁷ See Rule 4.4 Comment (“It is impractical to catalogue all such rights [of third persons], but they include legal restrictions on methods of obtaining evidence from third persons *and unwarranted intrusions into privileged relationships, such as the client-lawyer relationship.*” (emphasis added)). Arguably, the tracking device creates unauthorized “communications” between the client and opposing counsel in violation of Rule 4.2.

devices (whether disclosed or not) is dishonest and unethical. And, it is entirely possible that a busy receiving lawyer may not notice the disclosure, may not fully appreciate what it means, or consider whether client consent is necessary before agreeing (expressly or implicitly) to opposing counsel putting an electronic tracking device on documents.

The Committee notes that Rule 1.6(c) requires a lawyer to take “reasonable precautions” transmitting a communication that includes a client confidence or secret so as to avoid allowing the information to come into the possession of unintended recipients, including information in electronic form.⁸ The Committee does not interpret this duty as requiring the lawyer to presume that opposing lawyer will seek to “bug” communications and requiring the lawyer to take active steps to detect and prevent such tracking devices. As a practical matter, with rapidly changing technology and software that may be impractical or even impossible for the receiving lawyer to accomplish. The Committee believes that the only reasonable means of protecting attorney-client communications and work product in this situation is to bar the lawyer sending the communication from using these types of tracking devices.

The Committee therefore concludes that tracking electronic communications with opposing counsel through “web bugs” impermissibly and unethically interferes with the lawyer-client relationship and the preservation of confidences and secrets.⁹ Doing so reflects, at a minimum, the lack of straightforwardness that is a hallmark of dishonest conduct.¹⁰ Sending “bugged” emails or documents or other communications with embedded tracking devices constitutes an impermissible infringement on the lawyer’s ability to preserve a client’s confidences or secrets as required by Rule 1.6¹¹ and violates Rule 8.4(a) and (c).

Approved by the Alaska Bar Association Ethics Committee on September 1, 2016.

Adopted by the Board of Governors on October 26, 2016.

⁸ See Opinion No. 1998-02 (“Communication by Electronic Mail”) and Opinion 2014-03 (“Cloud Computing”).

⁹ See N.Y.S.B.A. Opinion 749 (2001) (finding that the surreptitious tracing of email and other electronic documents “would violate the letter and spirit” of the disciplinary rules, including rules prohibiting dishonest and deceptive conduct and rules relating to the protection of client secrets).

¹⁰ See, e.g., *Matter of Shorter*, 570 A.2d 760, 767-68 (D.C. Cir. 1990) (describing “dishonesty” as encompassing conduct evincing “a lack of honesty, probity or integrity in principle; [a] lack of fairness and straightforwardness” (quoting *Tucker v. Lower*, 434 P.2d 320, 324 (Kan. 1967))).

¹¹ Rule 1.6(a) (“A lawyer shall not reveal a client’s confidence or secret unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation and disclosures permitted by paragraph (b) below or Rule 3.3. ...”).