FORMAL OPINION 2017-300

ETHICAL OBLIGATIONS OF LAWYERS USING SOFTWARE TO TRACK EMAIL SENT TO OPPOSING COUNSEL

I. Introduction and Summary

An email tracker or "web bug" is a type of software that tracks who is reading an email or other electronic communication. Web bugs are commonly used by email marketers to determine who has opened an email, if it was forwarded, and to provide other information to the sender. Because the recipient of the email does not know whether the email contains a web bug, it is difficult, if not impossible, for the recipient to protect himself or herself.

The use of web bugs by an attorney to track the receipt and distribution of an email sent to opposing counsel raises the following ethical issues: (1) whether an attorney violates Rule 4.4 ("Respect for Rights of Third Persons") by impermissibly intruding into the client-lawyer relationship; and (2) whether an attorney violates Rule 8.4 ("Misconduct") by engaging in conduct involving dishonesty, deceit or misrepresentation for the purpose of obtaining client confidential information protected by Rule 1.6 ("Confidentiality"). It is this Committee's opinion that an attorney who knowingly employs web bugs under these circumstances violates Rule 4.4 by impermissibly intruding into the client-lawyer relationship, and Rule 8.4 by engaging in conduct involving dishonesty, deceit or misrepresentation for the purpose of obtaining client confidential information protected by Rule 1.6.

II. Background

A web bug, also called a "web beacon," "pixel tag," "clear GIF" and "invisible GIF," is software that allows e-mail senders to track the path a message takes, including when the email was opened, how long it was reviewed, how many times it had been viewed, the approximate location of the recipient, and the email address of any persons to whom the email is forwarded. Conversely, web bugs are commonly used in commercial email to track a variety of information, primarily who reads the email, who clicks on links displayed in the email, and who forwards the email. Services such as Constant Contact or Mail Chimp use this technology, but do so using prominently-displayed links and images so that they encourage users to click on the links with the understanding that they are doing so.

Web bugs can also be embedded in documents, and provide similar information to the person sending the document. Because a web bug tracks information as soon as an email is read, a recipient cannot "clean" the email until after the information has been provided to the sender. Moreover,

other than viewing email in text format (rather than in HTML, which displays images, etc.), which is not desirable to most users, it is impractical, if not impossible, for recipients to proactively protect themselves from web bugs.

The use of web bugs in other areas has raised legal concerns for many years. For example, in 2006, Hewlett-Packard revealed that its investigators were using web bugs to try to determine who was leaking confidential boardroom information.[1]

Because lawyers correspond with clients and opposing counsel by email, the ability of a sender to surreptitiously track how a recipient handles an email, *e.g.,* to track whether the recipient forwards the email, raises ethical concerns.

III. Discussion

A. Pennsylvania Rules of Professional Conduct

While no Pennsylvania Rule of Professional Conduct specifically addresses email tracking, the use of web bugs implicates several Rules, which address an attorney's responsibilities towards clients, potential clients, and other parties, including:

- Rule 1.6 ("Confidentiality of Information")
- Rule 4.4 ("Respect for Rights of Third Persons")
- Rule 8.4 ("Misconduct")

Rule 1.6 ("Confidentiality of Information") states in relevant part:

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

Comments [25] and [26] to Rule 1.6 require lawyers to act diligently to protect confidential client information, provided the lawyer has made reasonable efforts to prevent access to the information:

> [25] Paragraph (d) 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 (d) if the

[1] https://www.pcworld.com/article/127444/article.html

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 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].

[26] 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.

Rule 4.4 ("Respect for Rights of Third Persons") states in relevant part:

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

Comment [1] to Rule 4.4 provides:

[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 third persons. It is impractical to catalogue all such rights, 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.

Rule 8.4 ("Misconduct") states in relevant part:

It is professional misconduct for a lawyer to:

(a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another; …

(c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation;

B. Opinions of Other Ethics Committees

Two Ethics Committees have considered this issue and concluded that an attorney violates the Rules of Professional Conduct by using web bugs to track how a recipient handles an email.

The New York State Bar Association Committee on Professional Ethics issued Opinion 749 (December 14, 2001) in which it concluded that the use of "web bugs" and other email tracking methods is an impermissible intrusion into the confidential attorney-client relationship. The Committee stressed that in light of the strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship, the use of such technology to surreptitiously obtain information that may be protected by the attorney-client privilege, the work product doctrine, or may otherwise constitute a "secret" of another lawyer's client, would violate the letter and spirit of these Disciplinary Rules.

The Alaska State Bar Association Ethics Committee issued Opinion No. 2016-1 in which it concluded that email tracking is impermissible because it is considered professional misconduct and it interferes with the confidential attorney-client relationship. The Committee noted that the use of a tracking device that provides information about how a reader handles an email, aside from its receipt, violates Rule 4.4 and Rule 8.4, and also potentially impermissibly infringes on a lawyer's ability to preserve a client's confidences as required by Rule 1.6.

C. Analysis

Among an attorney's most basic obligations is to preserve attorney-client confidentiality. This obligation requires, for example, attorneys to take reasonable measures to assure that only clients view and participate in their communications. For example, when a lawyer receives a document in the mail from opposing counsel and forwards it to a client, the lawyer and the client may reasonably believe that the sender is not aware of that subsequent communication, including when and how it was transmitted, when the client viewed it, and when or if the client forwarded the document to another person. The use of web bugs is contrary to this assumption.

Thus, the use of web bugs violates Rule 4.4 to the extent that they permit the sending attorney to engage in unwarranted intrusions into confidential client relationships, such as the client-lawyer relationship, and Rule 8.4 to the extent that they permit the sending attorney to engage in conduct involving dishonesty, deceit or misrepresentation for the purpose of obtaining client confidential information protected by Rule 1.6. This Committee agrees with the New York and Alaska Opinions, both of which concluded that this duty does not require a lawyer to presume that an opposing lawyer will "bug" their communications and require the receiving lawyer to take proactive steps to detect and prevent such tracking devices.

The use of web bugs is different from the tracking of metadata, which this Committee discussed in PBA Formal Opinion 2009-100. Metadata is information contained within electronic files, such as comments and tracked changes in documents created in software such as Microsoft Word. In the case of metadata, the sending attorney has an obligation to review and, as necessary, remove any

relevant metadata to prevent opposing counsel from viewing it. Thus, the sender knows, or reasonably should know, that a document may contain this type of potentially confidential information. Conversely, it may be impractical or even impossible for a receiving lawyer to determine whether an email contains a web bug. This Committee therefore concludes that the only reasonable means of protecting attorney-client communications and work product is to bar a lawyer sending the communication from using these types of tracking devices.

The New York Opinion also noted that the use of these web bugs may violate federal law, which prohibits the unauthorized interception of e-mail content. *See, e.g.*, The Electronic Communications Privacy Act, 18 U.S.C. § § 2510, *et seq*. If a law bars the use of web bugs in attorney communications, an attorney may also be deemed to violate Rule 8.4(b), which states that it is professional misconduct for a lawyer to commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness or fitness as a lawyer in other respects.

Regardless of whether a law prohibits the use of web bugs, this Committee believes that their use violates Rule 8.4's prohibition against "conduct involving dishonesty, fraud, deceit or misrepresentation." Because the lawyer receiving the email does not and cannot reasonably determine or protect against web bugs, the sending lawyer's use of these devices would violate Rule 8.4. As in other contexts involving the Rules of Professional Conduct, a lawyer may not direct others, such as nonlawyer staff, to employ web bugs in communications with other persons in the course of a representation. *See* Rule 8.4(a).

This Opinion relates to the use of web bugs and similar devices, but does not prohibit the use of "Read Receipts" or "Delivery Receipts" or similar tools used by Microsoft Outlook and other email programs. Because recipients are aware of, and may configure their software to permit such receipts, to make their use optional, or to preclude their use, their use by lawyers does not violate the Rules of Professional Conduct. This Opinion also does not prohibit the use of email services, such as Constant Contact or Mail Chimp, because (1) they are mass emails, and not personal to a client matter; (2) those services display their links to encourage users to click on them; and (3) lawyers and other recipients are aware that they are clicking on the links. Conversely, recipients cannot know that the sender has embedded a web bug into the communication.

IV. Conclusion

This Committee concludes that the Pennsylvania Rules of Professional Conduct prohibit lawyers from using "web bugs" or any other method to track the receipt and distribution of email sent to opposing counsel. While the use of visible tracking devices such as those used in commercial email do not violate the Rules of Professional Conduct, the use of a web bug, which opposing counsel cannot determine is present, violates Rules 4.4 and 8.4.

CAVEAT: THE FOREGOING OPINION IS ADVISORY ONLY AND IS NOT BINDING ON THE DISCIPLINARY BOARD OF THE SUPREME COURT OF PENNSYLVANIA OR ANY COURT. THIS OPINION CARRIES ONLY SUCH WEIGHT AS AN APPROPRIATE REVIEWING AUTHORITY MAY CHOOSE TO GIVE IT.