# ISBA Professional Conduct Advisory Opinion

**Opinion No. 18-01**
**January 2018**

Subject: Communication with Client; Communication with Represented Person; Confidentiality; and E-mail.

Digest: A lawyer may not use tracking software in emails or other electronic communications with other lawyers or clients in the course of representing a client without first obtaining the informed consent of each recipient to the use of such software. It is not reasonable to require that lawyers acquire special devices or programs to detect or defeat tracking software.

References: Illinois Rules of Professional Conduct 1.1, 1.6, 1.9, 4.4, and 8.4

Illinois Supreme Court Rules 9(a); 11(d); 131(d); 201(p); and 756(c)(4)

ISBA Professional Conduct Advisory Opinions No. 95-10 (January 1996) and No. 98-04 (January 1999)

American Bar Association Formal Opinions 01-422 (June 24, 2001); 06-442 (August 5, 2006); 477R (May 22, 2017); and 479 (December 15, 2017).

Alaska Bar Association Ethics Opinion No. 2016-1 (October 26, 2016)

New York State Bar Association Opinion 749 (December 14, 2001)

720 ILCS 5/14-2 (2016)

## QUESTION

The inquiring lawyer asks whether the use of undisclosed "tracking" software (sometimes known as "web bugs," "web beacons," or "spymail") in emails or other electronic communications with other lawyers or clients is ethically permissible.

## ANALYSIS

## The Relevant Rules

The use of email and the exchange of documents in electronic form are necessary features of contemporary legal practice. An Illinois lawyer can no longer decide not to use email or to avoid dealing with electronic documents. See, e.g., Illinois Supreme Court Rule 9(a), which requires that all documents in Illinois civil cases be filed electronically with the clerk of court; Supreme Court Rules 11(d) and 131(d), which require that the appearance and all pleadings filed in court include an email address to which service may be directed; and Supreme Court Rule 756(c)(4), which requires that all Illinois lawyers complete the annual registration process online.

The Illinois Rules of Professional Conduct also address the use of electronic communications and documents. Comment [8] to Illinois Rule 1.1, as amended effective January 1, 2016, explains that in maintaining competence, "a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology…." A related provision, Paragraph (e) of Illinois Rule 1.6, adopted effective January 1, 2016, provides: "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." Comment [18] to Illinois Rule 1.6 explains:

> [18] 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. ... 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. 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).

Paragraph (b) of Illinois Rule 4.4, adopted effective January 1, 2016, provides: "A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows that the document or electronically stored information was inadvertently sent shall promptly notify the sender." Comment [2] to Illinois Rule 4.4 explains:

> [2] Paragraph (b) recognizes that lawyers sometimes receive a document or electronically stored information that was mistakenly sent or produced by opposing parties or their lawyers. ... If a lawyer knows that such a document or electronically stored information was sent inadvertently, then this Rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures. … For purposes of this Rule, "document or electronically stored information" includes, in

addition to paper documents, email and 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. Metadata in electronic documents creates an obligation under this Rule only if the receiving lawyer knows that the metadata was inadvertently sent to the receiving lawyer.

**Discussion**

The present inquiry involves the use of email "tracking" software, applications that permit the sender of an email message to secretly monitor the receipt and subsequent handling of the message, including any attachments. [1] 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. There do not appear to be any generally available or consistently reliable devices or programs capable of detecting or blocking email tracking software.

Illinois Rule 8.4(a) provides that it is professional misconduct for a lawyer to "violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another." Rule 8.4(c) provides that it is also professional misconduct to "engage in conduct involving dishonesty, fraud, deceit, or misrepresentation." The New Oxford American Dictionary (3d ed. 2010) defines "dishonesty" to mean "deceitfulness shown in someone's character or behavior" (at p. 498) and "deceit" to mean "the action or practice of deceiving someone by concealing or misrepresenting the truth" (at p. 448).

The undisclosed use of email tracking software by a lawyer, without the informed consent of the recipient, conceals the fact that the sending lawyer is secretly monitoring the receipt and handling of the email message and its attachments by the original recipient as well as each subsequent receiving party. Any competent lawyer receiving an email from an opposing counsel would obviously wish to know that the opposing counsel is acquiring instantaneous and detailed private information concerning the opening and subsequent handling of the email and its

[1] Tracking software is apparently used in various commercial settings, ostensibly to gauge the effectiveness of marketing materials. Many email programs offer a "read-receipt" function, an electronic analogy to certified mail, that gives a recipient the option to notify the sender that an email was received. Because this function provides only a confirmation of receipt rather than information concerning the subsequent handling of an email, it does not appear to raise the client protection concerns discussed in this opinion.

attachments. At a minimum, concealing the use of tracking software constitutes "dishonesty" and "deceit" within the meaning of Illinois Rule 8.4(c).

More fundamentally, this type of deception, if used in email correspondence with another lawyer in the course of representing a client, covertly invades the client-lawyer relationship between the receiving lawyer and that lawyer's client. Alaska Bar Association Ethics Opinion No. 2016-1 (October 26, 2016) cites two persuasive examples of such interference. The first involved a client who had moved and did not want her new location disclosed. If opposing counsel sends her lawyer a tracked email attaching a document for her review or signature, the tracking software will reveal the client's general location when she opens the forwarded email with the document. The second example involved a tracked email attaching a proposed settlement agreement. In that case, the tracking software would reveal to the sending lawyer the pages of the proposal that the receiving lawyer and client reviewed, as well as how often and how long each reviewed any particular page of the proposal. As the Alaska opinion noted, the use of such software gives the sending lawyer access to "protected information and extraordinary insight as to which sections of a document the lawyer and her client found most important." The Alaska opinion concluded that the use of tracking software impermissibly and unethically interferes with the client-lawyer relationship and the protection of client information. [2]

In addition to those noted in the Alaska opinion, numerous other opportunities for intrusion into the representation of a client could arise from the monitoring of email communications between the receiving lawyer and others involved in the representation, including: insurers, co-counsel, co-clients, expert witnesses, consulting experts, accountants, investigators, and other nonlawyer service providers. The fact and details of these types of communications are confidential information relating to the representation of a client or former client, information protected by Illinois Rules 1.6(a) and 1.9(c)(2) from disclosure by the lawyer representing those clients. [3] As such, covertly obtaining this protected confidential information should be considered the type of unwarranted intrusion into the client-lawyer relationship condemned in Comment [1] to Illinois Rule 4.4(a). Rule 4.4(a) provides that a lawyer shall not use methods of obtaining evidence that violate the rights of a third person; and Comment [1] explains: "It is impractical to catalogue all such rights, but they include … unwarranted intrusions into privileged relationships, such as the client-lawyer relationship." [4]

The undisclosed use of tracking software is closely analogous to the surreptitious recording of telephone calls. In Formal Opinion 01-422 (June 24, 2001), the American Bar Association reversed a prior long-standing opinion to hold that recording a telephone

---

[2] See also New York State Bar Association Opinion 749 (December 14, 2001), concluding that "in light of the strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship, use of technology [web bugs] to surreptitiously obtain information that may be protected … would violate the letter and the spirit" of the New York Rules.

[3] See, e.g., ABA Formal Opinion 479 (December 15, 2017).

[4] Paragraph [2] of the Preamble to the Illinois Rules: "As negotiator, a lawyer seeks a result advantageous to the client but consistent with requirements of honest dealings with others." See also *In re Neary*, 84 N.E.3d 1194 (Ind. 2017) (four-year suspension of prosecutor who violated Indiana Rules 4.4(a) and 8.4(d) by eavesdropping on two private client-lawyer conversations).

conversation without the knowledge of the other party to the conversation does not necessarily violate the ABA Model Rules.[5] ABA Formal Opinion 01-422 also stated, however, that a lawyer could not record telephone conversations in violation of the law in a jurisdiction that forbids such conduct without the consent of all parties, nor falsely represent that a conversation is not being recorded. In Illinois, secretly recording a private telephone conversation without the consent of all parties to the conversation violates state law, unless certain specific exceptions apply. See 720 ILCS 5/14-2(a)(2) (2016).[6] N6. As a result, non-consensual recording of telephone calls likely also violates Illinois Rules 8.4(b) or 8.4(c), or both. The Illinois public policy against covert recording of telephone calls further suggests that the undisclosed tracking of email messages should be considered conduct involving dishonesty or deceit.

The undisclosed use of tracking software is contrary to the rationale of Illinois Rule 4.4(b). As noted above, that rule provides that 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. Comment [2] to Rule 4.4 explains that the purpose of requiring a lawyer who receives an inadvertent communication to promptly notify the sender is "to permit that person to take protective measures." Comment [2] also confirms that the rule extends to email and other forms of electronically stored information. If the professional conduct rules require lawyers to promptly notify the sender when client confidential information is received by inadvertence, to permit the sender to take protective measures, then those rules should not be interpreted to permit lawyers to procure the same type of information by stealth.[7]

The undisclosed use of tracking software is also inconsistent with prior ISBA Opinions. For example, ISBA Opinion No. 98-04 (January 1999), issued before the 2016 adoption of Rule 4.4(b), concluded that a lawyer who learns of the inadvertent transmission of an opposing party's confidential materials before those materials have been opened and reviewed should return such materials without examination. ISBA Opinion No. 98-04 observed that "reading inadvertently produced material after learning of the error is similar to copying papers from an opposing lawyer's file folders during a break in a deposition. Such conduct has been found to be dishonest. It would also be considered a form of 'sharp practice' condemned by this Committee in Illinois Opinion No. 95-10 (January 1996)." If it is improper for a lawyer to read confidential information of another party that has been disclosed by inadvertence, then it is improper for a lawyer to obtain such information through the covert use of tracking software.

---

[5] The ABA opinion justified its reversal primarily on the observation that in 2001: "it is questionable whether anyone today justifiably relies on an expectation that a conversation is not being recorded by the other party, absent a special relationship with or conduct by that party inducing a belief that the conversation will not be recorded."

[6] For an analysis of the Illinois Eavesdropping Act, see *The Two Faces of Eavesdropping*, 103 Illinois Bar Journal, No. 6, p. 20 (June 2015).

[7] See also Illinois Supreme Court Rule 201(p), which provides that after a lawyer is notified that inadvertently produced information is subject to a claim of privilege or work-product protection, the lawyer must "promptly return, sequester, or destroy" the specified information and must not use or disclose the information until the claim of privilege is resolved.

Although Comment [8] to Illinois Rule 1.1 and Illinois Rule 1.6(e), express a general duty that a lawyer should keep abreast of the benefits and risks associated with relevant technology as well as make "reasonable efforts" to prevent unauthorized access to client information, requiring the receiving lawyer to first discover and then defeat every undisclosed use of tracking software would be unfair, unworkable, and unreasonable.

It would be unfair for at least two reasons. First, it is unfair to require lawyers to use email and other electronic documents in communications regarding their practice and then interpret the professional conduct rules to enable the undisclosed use of tracking software to gain covert, unauthorized access to protected client information of opposing parties. Second, it is unfair to require lawyers receiving email, i.e., all lawyers, to assume that all email messages contain undisclosed tracking software because that approach places the burden of preventing unauthorized access to protected client information on the wrong party. The sending lawyer is the actor in these situations and controls whether, when, and what type of tracking software to employ. Tracking software is not, for example, a common functional aspect of electronic documents like metadata. As noted in ABA Formal Opinion 06-442 (August 5, 2006), metadata is embedded information that enables word-processing software to manage documents and facilitates collaborative drafting among colleagues. Unlike tracking software, which must be purposely, and usually surreptitiously, inserted into an email, metadata is a universal feature of every word-processed document. It is appropriate and reasonable to expect lawyers to understand metadata and other ubiquitous aspects of common information technology.[8] But it would be neither appropriate nor reasonable to charge all lawyers with an understanding of the latest version of tracking software that might be chosen, and then employed without notice, at the option of opposing counsel.

Even assuming that "defensive" software or devices capable of discovering and/or defeating tracking software were to become available, it would be unworkable to, in effect, force every Illinois lawyer to become and remain familiar with the various tracking programs on the market and then immediately purchase and install whatever new anti-tracking software or device that may, or may not, protect against the latest version. Given the typical rapid changes in technology, few, if any, solo or small firm lawyers could reasonably do so. Aside from creating sustained employment for IT consultants and software vendors, that approach would only precipitate an "arms race" in which the developers and users of tracking software would always be a step ahead.

## Conclusions

As explained in Comment [18] to Rule 1.6, the cost and difficulty of implementing additional safeguards to protect client information are factors in determining the reasonableness of a lawyer's efforts. In this context, the cost and difficulty of discovering and/or defeating tracking software make it unreasonable to place the burden of protecting client information from the use of tracking software on the receiving lawyer. The most realistic, effective, and reasonable

[8] See, e.g., ABA Formal Opinion 477R (May 22, 2017).

way to protect client information in this context is to prohibit the use of tracking software in email correspondence with another lawyer in the course of representing a client.[9]

Accordingly, if a lawyer wishes to use tracking software in email correspondence with another lawyer in the course of representing a client, the sending lawyer must receive prior informed consent to such use.[10] Any email seeking such consent must (1) itself be free of tracking software; (2) contain no other substantive content; and (3) give the recipient a clear, explicit, and non-technical plain language explanation of the features of the particular software that the sending lawyer proposes to use.[11] Before agreeing to accept email correspondence regarding the representation of a client that may contain tracking software, the receiving lawyer should also obtain the informed consent of any affected client.

The concerns that make the undisclosed use of tracking software in email involving other lawyers improper apply with equal, and perhaps greater, weight to email correspondence with clients. The client-lawyer relationship is one of trust and confidence.[12] N12. As stated in ABA Formal Opinion 01-422: "Lawyers owe to clients, unlike third persons, a duty of loyalty that transcends the lawyer's convenience and interests." For that reason, ABA Formal Opinion 01-422 concluded that a lawyer should "almost always" inform a client that a conversation is or may be recorded. For the same reason, a lawyer should never use tracking software in email correspondence with a client without first obtaining the client's informed consent. If a lawyer reasonably believes that using tracking software in email correspondence with a client serves the client's interests, there should be no difficulty obtaining informed consent to such use. If the client declines to consent to receiving tracked email, the lawyer must honor that decision.



---

[9] As Alaska Opinion No. 2016-1 noted: "As a practical matter, with rapidly changing technology and software … [detecting tracking devices] 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."

[10] There may be situations where a lawyer's use of tracking software does not implicate client interests or otherwise involve the representation of a client, such as in email correspondence concerning a lawyer's own business activities. This opinion does not address those situations.

[11]The general definition of "informed consent" under Illinois Rule 1.0(e) denotes "… the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct."

[12] Comment [1] to Illinois Rule 1.8 observes that the requirements applicable to business transactions between client and lawyer derive from the "… relationship of trust and confidence between lawyer and client …." This is a long-standing and essential element of the client-lawyer relationship: "There are few of the business relations of life involving a higher trust and confidence than that of attorney and client … or governed by sterner principles of morality and justice …." *Stockton v. Ford*, 52 U.S. 232, 247 (1850).