

November/December 2018

# The Bencher<sup>®</sup>

THE MAGAZINE OF THE AMERICAN INNS OF COURT<sup>®</sup>



# TECHNOLOGY

[www.innsocourt.org](http://www.innsocourt.org)





# TECHNOLOGY IN THE PRACTICE OF LAW

Kevin F. Brady, Esquire

## Email Tracking Software

Did you ever want to track an email that you sent just to see where it goes? Businesses use email tracking software to monitor the receipt and subsequent handling of the message. Email tracking software uses certain features, such as “web beacons,” “web bugs,” or “spymail” to collect analytics such as: was the email opened (and if so what was the IP address), on what type of device was it opened, how long was it opened before it was closed or deleted, and was a link clicked from inside the e-mail. If businesses are permitted to use surreptitious tracking software in emails or other electronic communications, may lawyers use that software with other lawyers or clients without running afoul of the Rules of Professional Responsibility?

A Professional Conduct Advisory Opinion issued by the Illinois State Bar Association in January 2018 (Opinion No. 18-01) (following similar opinions from New York, Pennsylvania, and Alaska) answered the question with a resounding “No.” The Illinois Opinion explained:

*[T]racking 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. Op. at 3.

Even assuming that such software was readily available, the opinion concludes that it would be unreasonable to force every lawyer to be familiar with those various tracking programs and implement them into their practice. “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.” *Id.*

Moreover, while Comment 8 to the ABA Model Rules requires lawyers keep abreast of the benefits and risks associated with relevant technology, and ABA Model Rule 1.6(c) requires lawyers to make reasonable efforts to prevent inadvertent or unauthorized access to client information, the opinion notes that “requiring the receiving lawyer to first discover and then defeat every undisclosed use of tracking software would be unfair, unworkable, and unreasonable.” *Id.*

The opinion is clear that the *undisclosed* use of email tracking software by an attorney without the informed consent of the recipient, at a minimum, constitutes “dishonesty” and “deceit” within the meaning of Illinois Rule 8.4(c) and... “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.” *Id.* at 3-4. The opinion did note that email programs that offer a “read-receipt” function that gives a recipient the option to notify the sender that an email was received are allowed. Because this function provides only a confirmation of receipt rather than information concerning the subsequent handling of an email, the opinion distinguished the “read-receipt” option from the email tracking software noting that, “it does not appear to raise the client protection concerns...” Op. at 3.

While many jurisdictions have not issued any specific guidance on this topic, lawyers should be aware of the existence of this technology and the non-binding opinions for any jurisdiction that follows the Model Rules of Professional Conduct. ♦

Kevin F. Brady, Esquire, is of counsel in the Washington, DC firm of Redgrave LLP. He is a past president of the Richard K. Herrmann Technology Inn in Wilmington, Delaware and a member of the American Inns of Court Leadership Council.