Bloomberg BNA | ABA

ABA/BNA
Lawyers' Manual on Professional Conduct™

Email tracking tools are spreading like wildfire. Here's what legal professionals need to know.

Email Tracking: Is It Ethical? Is It Even Legal?

By Chad Gilles

Introduction

Email tracking using invisible ''web bugs'' (or ''beacons'') is now ubiquitous. Web-bugged emails invisibly reveal information such as:

- when and how often an email is opened;
- where and on what device an email is opened; and
- whether and where an email has been forwarded.

This covert extraction of sensitive information has earned email tracking the moniker ''spymail.''

Email tracking tools from companies such as Salesforce, Hubspot, Yesware, Streak, Bananatag, ReadNotify, and dozens of others are cheap and simple to use for even the most technologically challenged. As a result, millions of people now use them to track what recipients do with their emails.

Attorneys are among both the senders and recipients of such spymail. At MailControl we see this first hand—attorneys tracking attorneys, attorneys tracking clients, clients tracking attorneys, clients tracking opposing parties, cyber criminals tracking attorneys and clients . . . you name it. Email tracking has come up in court opinions such as *Pashman v. Aetna Ins. Co.*, 2014 BL 199793, No. C-13-02835 DMR, at 33 n.14 (N.D. Cal. July 18, 2014) (describing how defendant's employee ''used an email tracking service to confirm that Plaintiff received and opened the . . . email'' and to conclude that plaintiff ''had forwarded the termination email'' to a particular law firm). Email tracking was also directly addressed by a recent Alaska Bar Association ethics opinion. Alaska Ethics Op. 2016-1, 32 Law. Man. Prof. Conduct 638 (10/26/16).

How should attorneys deal with spymail in their practice? This article first looks at how email tracking works. It then discusses both whether attorneys can use email tracking ethically, and how attorneys can lessen the risks that email tracking presents to their clients and themselves.

Chad Gilles handles customer strategy and legal affairs for MailControl.net. Prior to MailControl, Chad worked for nine years as a patent agent/attorney and three years as an electrical engineer. To contact him: chad.gilles@mailcontrol.net.

How Does Email Tracking Work?

Email tracking typically relies on tracking code that is embedded in an email message and that gets automatically triggered upon the email being opened. As described in the Alaska ethics opinion, a common form of tracking code is:

> an image with a unique address on an Internet server, and the image is either invisible or disguised as part of the [email]. When the recipient opens the document, the recipient's computer looks up the image and thereby sends certain information to the sending party.

 ISSN 0740-4050

The internet server to which the information is sent is typically owned by the tracking tool provider. The tracking tool provider then makes the data available to the sender—typically through a ''dashboard'' or ''app.''

The information extracted from the recipient's computer includes its IP Address and its hardware and software configuration (e.g., browser type and operating system version). The IP Address can be cross-referenced with various databases to reveal the recipient's location, among other things. The information from the recipient's computer may also come from cookies previously planted on the machine (e.g., by an earlier web bug). These cookies can transmit more-detailed information about the recipient, such as her identity and web browsing history.

Reasonable Minds Disagree on the Ethics of Email Tracking

Until the Alaska opinion, the only formal ethics opinion to address the issue of spymail had been a 2001 opinion from the New York State Bar Association, which reached a similar conclusion. N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 749, 12/14/2001. And while there was a 15-year gap between those opinions, it wouldn't be surprising for the pace to pick up, given the rapid increase in the number of web bugs in a typical attorney's inbox.

''It should be self-evident to any lawyer who has taken a law-school ethics course or an ethics CLE that bugging e-mail sent to opposing counsel is dishonest.''

Karen Rubin, Thompson Hine

But it's not clear that other bar ethics panels would—or should—reach the same conclusion as Alaska and the NYSBA.

Some attorneys see email tracking as clearly unethical. Thompson Hine attorney Karen Rubin, for example, wrote that ''[i]t should be self-evident to any lawyer who has taken a law-school ethics course or an ethics CLE that bugging e-mail sent to opposing counsel is dishonest.''

Similarly, Lewis Thomason attorney Brian Faughnan opined that ''the [Alaska] opinion is pretty well done and reaches the obvious and correct solution.''

Other attorneys take the opposite view. Ethics professor Dane Ciolino, for example, has written that:

> Every day lawyers receive emails embedded with tracking bugs and read-receipts. There is nothing 'fraudulent,' 'deceitful,' or 'dishonest' about sending such emails. They are commonplace. Considering this, the burden should be on the lawyer-recipient to make sure that privileged and confidential information is not reported back to a sender.

''Every day lawyers receive [tracked] emails. There is nothing 'fraudulent,' 'deceitful,' or 'dishonest' about sending such emails. They are commonplace.''

Dane Ciolino, ethics professor

This view—that the burden should be on the recipients to guard against spymail—is one also pondered by Vermont bar counsel Michael Kennedy. In commenting on the Alaska Bar Association's statement that Rule 1.6(c) (duty to take ''reasonable precautions'' against inadvertent disclosure of confidential information) does not impose a duty to actively guard against email tracking, Mr. Kennedy weighed in that Alaska's view is:

> quite different from the evolving view of a lawyer's duties with respect to the electronic storage and transmission of client information. It's also the exact opposite of what we're telling lawyers with respect to metadata & track changes. With metadata & track changes, we've clearly stated that it's perfectly okay to look for information that goes to the heart of the attorney-client relationship. In so doing, we've said that if you don't know about metadata and don't take steps to prevent it from being accessed, it's your problem, not the lawyer's who looks for it without telling you that she's looking.

Given these differing positions, it makes sense to take a closer look at the NYSBA and Alaska opinions.

New York State Bar Association Opinion #749

Though on the surface the N.Y. opinion seems to say that attorneys cannot ethically send web-bugged emails, a closer reading shows more nuance. First, the N.Y. opinion conflates metadata and email tracking, and ethics panels have softened considerably on metadata in the interim. Second, technology has changed a lot since 2001, rendering some of the opinion's factual assumptions inaccurate.

The first paragraph of the opinion covers ''information that the sender has not intentionally made available,'' such as where ''a lawyer who has received the final draft of a contract from counsel for a party with whom the lawyer is negotiating would be able to see prior drafts of the contract and, perhaps, learn the identity of those who made the revisions, without the knowledge or consent of the sending lawyer.'' This clearly describes metadata, not information that an email-embedded web bug can provide.

The second paragraph describes a web bug in an email that can reveal ''the subsequent route of the e-mail, including comments on the e-mail written by its ultimate recipients.'' While web bugs in emails can reveal the identity of subsequent recipients, the opinion is wrong in stating they can reveal subsequent comments.

Also, although the N.Y. opinion's statement that ''it is virtually impossible to render one's e-mail system 'bug-proof' '' may have been true in 2001, technology has advanced to the point where it is no longer accurate.

The N.Y. opinion then formulates the question presented as ''may a lawyer ethically may [sic] use avail-

  MOPC ISSN 0740-4050

able technology to surreptitiously examine and trace e-mail and other electronic documents in the manner described?''

In answering that question in the negative, the N.Y. opinion cites N.Y. Disciplinary Rule 1-102(A)(4) (now Rule 8.4(c)), which prohibits conduct ''involving dishonesty, fraud, deceit or misrepresentation,'' and Disciplinary Rule 1-102(A)(5) (now Rule 8.4(d)), which prohibits ''conduct that is prejudicial to the administration of justice.'' The N.Y. opinion states:

> [I]n light of the strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship, use of technology to surreptitiously obtain information that may be protected by the attorney-client privilege, the work product doctrine or that may otherwise constitute a ''secret'' of another lawyer's client would violate the letter and spirit of these Disciplinary Rules.

But the N.Y. opinion relies on authority that has since been revoked or called into question. It cites ABA Formal Op. 92-368 (the ''misdirected fax'' opinion), which held that ''a lawyer who receives confidential materials under circumstances where it is clear that they were not intended for the receiving lawyer (a) should not examine the materials once the inadvertence is discovered, (b) should notify the sending lawyer of their receipt, and (c) should abide by the sending lawyer's instructions as to their disposition.'' Opinion 92-368, however, was formally withdrawn in ABA Formal Opinion 05-437, in which the ABA sided with several other states (including CO, MD, MN, OR, PA, VT, WA, and WI, according to the ABA's collection of metadata opinions) that deemed the mining of metadata to be ethically permissible.

In jurisdictions that (unlike New York) permit metadata mining, much of the reasoning of the N.Y. opinion is inapplicable. Such states may be more likely to find that the burden is on the email recipient to guard against inadvertently disclosing confidential information through opening and/or forwarding web-bugged emails.

A few additional points are worth noting. First, the N.Y. opinion only addresses ''surreptitious'' web bugs—not those the sender plainly discloses. Second, the opinion says it is unethical to use surreptitious email tracking for gathering information that is attorney-client privileged or protected by the work product doctrine. It is unclear whether a hidden web bug solely for read notification falls under this category.

Alaska Bar Association Opinion 2016-1

The Alaska opinion concludes it is not ''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.'' It states that ''[t]he 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.''

''[Alaska's opinion that there is no duty to guard against web bugs is] the exact opposite of what we're telling lawyers with respect to metadata & track changes.''

Michael Kennedy, Vermont Bar Counsel

In reaching its conclusion, the Alaska opinion relies on two lines of reasoning. The first is that attorneys can reasonably assume their emails are not bugged. The second is that email tracking potentially intrudes on the attorney-client relationship.

On the first point, the opinion analogizes web bugs to the recording of telephone conversations by attorneys in the 1970s. The Committee writes that:

> [an] 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. Given that assumption, a lawyer who recorded a conversation without giving appropriate notice or obtaining consent had engaged in misrepresentation or deceit. 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.
>
> 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 ''bugged.'' And, consistent with Opinion 88-4, the Committee likewise believes that it is unethical to use tracking devices on electronic communications.

Implicit in this reasoning is that the ethical propriety of a technology depends on its prevalence. This begs the question: at what point do web bugs transition from being ''1970s telephone recording technology'' to being ''2003 telephone recording technology?'' Given that there are dozens of email tracking tools, that millions of people are using these tools, and that there are thousands of tracked emails in the average attorney's mailbox, arguably that point has already passed. The Alaska Bar Association's position that there is a ''reasonable expectation that email is not bugged'' grows less tenable by the day.

The second—and more well-reasoned—prong of the Alaska opinion's argument is that the use of web bugs by opposing counsel potentially intrudes on the attorney-client relationship and the work product doctrine. As in New York State Ethics Op. 749, some of the examples given only apply to attachment metadata and not email web bugs. Of the remainder, those that involve information that can be gleaned from a web-bugged email are: (1) ''location of the recipients;'' (2)

''how much time the receiving lawyer spent reviewing the [email];'' (3) ''how frequently the communication was viewed (a proxy for how important the receiving lawyer deemed it to be);'' and (4) ''whether and when it was forwarded either to the client or co-counsel or otherwise.''

The Alaska opinion states,

> ''Seeking to invade [the attorney-client] relationship through the use of tracking 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.''

This quote is interesting in that (a) the ''seeking to invade'' language seemingly introduces an intent requirement; and (b) it goes against the prevailing trend of requiring attorneys to be technologically competent.

An intent requirement is also reflected in the opinion's express permission of web bugs for ''receipt and having been 'read' by opposing counsel.'' It may follow that the ethicality of any given web bug depends on what the sender intended when planting the web bug. Such intent would have to be determined by how the sender ultimately used the gathered information because, technologically speaking, there is no such thing as an ''only-for-read-notification'' web bug. All web bugs gather at least IP address and client type from the recipient if the recipient does not have technological barriers in place.

By prohibiting even disclosed web bugs because ''a busy receiving lawyer may not notice the disclosure, [or] may not fully appreciate what it means,'' the Alaska bar is at odds with the increasing adoption of Model Rule 1.1 comment [8], which requires ''keeping abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.'' And, in case this statement left any doubt, the opinion effectively absolves Alaska attorneys of responsibility for protecting clients against web bugs in stating:

> 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. 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.

Placing the onus on opposing counsel is ''the only reasonable means of protecting attorney-client communications and work product in this situation,'' the opinion argues.

''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.''
Alaska Ethics Opinion 2016-1

But how would this protect client confidences from web bug senders who aren't attorneys bound by the rules of professional conduct? Or, for that matter, from ''dishonest and unethical'' attorneys? A better approach would be to encourage attorneys to be on guard for spy-mail, regardless of the source.

Is Email Tracking Illegal and Thus Per Se Unethical?

Perhaps the most interesting part of the N.Y. opinion comes near the end:

> Although our jurisdiction does not extend to questions of law, we note that the misuse of some aspects of this technology, particularly the use of e-mail ''bugs,'' may violate federal or state law prohibiting unauthorized interception of e-mail content. See, e.g., The Electronic Communications Privacy Act, 18 U.S.C. § § 2510 et. seq. In that event, such conduct would, of course, be unethical per se.

In addition to Titles I-III of the ECPA, the Computer Fraud and Abuse Act (18 U S.C. § 1030) also contains potentially relevant provisions.

But surprisingly, there are few indications of anyone seriously questioning whether email tracking runs afoul of these laws. The consensus seems to be, ''if everyone is doing it, and no one has gotten in trouble, it must be legal.'' In fact, this argument was raised by a party in *Harrison Scott Publ'g v. Entrust Capital Mgmt.*, 14-cv-7052 GHW, Mot. at 8, Jan. 26, 2015 (S.D.N.Y) (''Careful scrutiny is particularly appropriate in this case. CFAA has been in effect since 1986 and ReadNotify has been in commercial use since at least the early 2000s. Yet a Westlaw word search does not reveal a single case in which use of ReadNotify has been asserted or held to violate the CFAA.''). Unfortunately, the case settled before the court addressed the issue.

The following brief overview highlights a number of unknowns that these statutes present with respect to email tracking.

Title I of the ECPA

Using web-bugged emails to detect when and where an email is forwarded may be a violation of Title I of the ECPA.

Title I of the ECPA provides criminal sanctions and a private right of action against ''whoever (1) intentionally (2) intercepts, endeavors to intercept or procures another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) us-

  MOPC ISSN 0740-4050

ing a device.'' *In Re Pharmatrak, Inc. Privacy Litig.*, 292 F. Supp.2d 263 (D. Mass. 2002).

While there is no case directly addressing whether Title I applies to web bugs in emails, some cases have addressed web bugs embedded in web sites. See, e.g., *Pharmatrak*; *In Re DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001); and *Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153 (W.D. Wash. 2001).

These cases seem to establish that one of the biggest questions as to the legality of web-bugged email under Title I is whether one party to the communication has consented to the use of the web bug. It is unlikely the original transmission of a web-bugged email would violate Title I since the sender who planted the web bug likely consented to its use (even if she didn't understand the tracking tool's terms of use). Where the original recipient forwards the web-bugged email to a second recipient, however, the tracking tool eavesdrops on that communication despite the fact that neither the original recipient nor the second recipient have consented.

In this case of an unknowingly-forwarded spymail, there is still the question of whether the interception was of the ''contents'' of the electronic communication. The statute defines the contents as ''any information concerning the substance, purport, or meaning of that communication.'' Interception of an email web bug would seem to meet this criterion because the sender knows the content of the forwarded email. That is, the sender does not simply learn the mere fact of a communication between the original recipient and the second recipient, but rather learns of a communication that is about and contains the content of the original email.

Title II of the ECPA

Web bugs in email probably do not violate Title II of the ECPA.

Title II of the ECPA provides for criminal punishment and a civil right of action against ''whoever (1) intentionally accesses without authorization a facility through which an electronic information service is provided; or intentionally exceeds authorization to access that facility; and thereby obtains . . . access to a wire or electronic communication while it is in electronic storage in such a system.''

As Title II applies to web-bugged email, the critical issue seems to be the definition of ''electronic storage.'' The tern ''electronic storage'' in Title II has usually been interpreted very narrowly to mean only temporary storage made in the course of transmission by a service provider and to backups of such intermediate communications made by the service provider to ensure system integrity. Email that has been received by the recipient's service provider but has not yet been accessed by the recipient is in ''electronic storage.'' See *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 461 (5th Cir. 1994) (email stored on provider's hard drive determined to be in ''electronic storage'').

Once the recipient retrieves the email, however, the communication has reached its final destination; if the recipient chooses to keep a copy on the email server, it will not be in ''electronic storage.'' See *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2004) (email in question had already been received by intended recipient so was no longer ''in transit'' and thus not in ''electronic storage''). So, under this traditional view of ''electronic storage,'' it would seem unlikely that a web bugged email would be a violation of Title II. The Ninth Circuit has adopted a broader interpretation of ''electronic storage'' that extends protection to previously-accessed emails still stored on the email server. But even in the Ninth Circuit, an email web bug would not seem to be a violation of Title II because the web bug is only triggered by the recipient-accessed copy of the email (not the copy ''backed up'' on the email server).

Title III of the ECPA

Using web-bugged emails to detect when and where an email is forwarded may be a violation of Title III of the ECPA.

Title III of the ECPA prohibits the use of pen registers and trap and trace devices (with numerous exceptions for law enforcement). A ''pen register'' is defined as:

> a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication . . .

A ''trap and trace device'' is defined as:

> a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however that such information shall not include the contents of any communication.

''Because Internet headers contain both 'to' and 'from' information, a device that reads the entire header (minus the subject line in the case of email headers) is both a pen register and a trap and trace device, and it is commonly referred to as a pen/trap device.'' Dep't of Justice, Criminal Division, Computer Crime and Intellectual Property Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 154 (2009).

Here the issues seem to be the same as for Title I. In the case of the original recipient forwarding a spymail to a second recipient, there would seem to be no consent to the collection of information via the web bug and thus Title III is violated.

Computer Fraud and Abuse Act

Using web-bugged emails to detect when and where an email is forwarded may be a crime under the CFAA, but the issue is unresolved.

The CFAA makes it a crime to intentionally access a computer without authorization, or exceed authorized access, and thereby obtain information from any protected computer if the conduct involved interstate or foreign communication. The CFAA also provides a civil right of action to ''any person who suffers damage or loss by reason of a violation of'' the statute. This ''damage or loss'' requirement has been interpreted very narrowly.

The biggest issues with respect to email web bugs and the CFAA seem to be: (1) whether an ''access'' has occurred, and, if so, (2) whether there was consent (i.e., authorization) for the access. Unfortunately, there is little guidance on these issues. Although *Chance*, *DoubleClick*, and *In re Intuit Privacy Litig.*, 138 F. Supp.2d 1272 (C.D. Cal. 2001) all looked at whether

web bugs can violate the CFAA, these three civil actions were dismissed for failing to meet the ''damage or loss'' requirement without addressing the other elements of the statute.

As for the ''access'' element, the statute does not provide an explicit definition. That said, *Chance*, *DoubleClick*, and *In re Intuit* all seem to take for granted that retrieving a cookie from a computer is an ''access'' of that computer. If obtaining a cookie is an ''access,'' obtaining a web bug should also be an ''access.'' This is because web bugs and cookies are both just strings of text that are stored in a recipient's computer and that are sent in an HTTP GET or POST request as instructed by the party who planted them.

Regarding the ''consent'' element, as with the ECPA, the case in which an original recipient unknowingly forwards a web bug to a second recipient seems to be most likely to result in a violation. In that scenario, the second recipient clearly has not consented to the sender and/or tracking tool provider obtaining information from his or her computer.

Don't Get Bitten

In sum, attorney use of email web bugs simply for read notification is probably neither unethical nor illegal. But email tracking beyond simple read notification does seem to be questionable from an ethical standpoint. And though there isn't any controlling authority, use of email tracking to discover when and where emails are forwarded could possibly be a crime.

Putting ethics aside, there are millions of users of these tools who are not bound by rules of professional conduct, and many who won't be deterred by criminal laws. The safest course is to assume all of your emails are bugged and act accordingly. Attorneys and clients alike would benefit from a ''buyer beware'' approach, as many states have adopted with respect to metadata.

  MOPC ISSN 0740-4050