

Mining for metadata: ethics questions surrounding inadvertently sent embedded data

Remember when you worried about what to do if you received an inadvertently sent fax from opposing counsel? This conundrum has been dressed up in a set of 21st century clothes – metadata. You hear the word everywhere these days. What is it? Technically, it is data about data. Virtually every digital document contains data behind the document that reveals things about it, like when it was created, who created it, when it was edited, how long it was worked on, and perhaps its history of editing changes. This is metadata. Digital documents can contain other somewhat hidden data. Technically not metadata, this information is simply document data that is embedded within the obvious document text. One example is comments about the document inserted by the author or others. In this article, I will refer to both types of information as embedded data.

Nightmares at the law office

Let's say you're late getting interrogatory answers to opposing counsel, so you e-mail them as a Word attachment to the other lawyer with an executed hard copy to follow by regular mail. These are the answers you had earlier e-mailed to your client to review. Your client returned them with several comments using the "insert comments" feature in Word. Your opponent selects the "display comments" feature, and there in the margin are your client's comments to you; like, the one that says: "Do we have to tell them that I'd been having brake problems for a couple of weeks before the accident?" *Oops!*

Or maybe you e-mail a document to your client, and you follow up with a bill for 2.5 hours of drafting time. When your client exam-

ines the "file properties" screen, she sees that the total time the document has been open is .3 hours. You created the document by recycling a preexisting document. You call it "quality billing." Your client probably calls it something else unsuitable for a family publication (raising more ethical issues for another day). *Oops!*

You send a summary judgment brief as a Word attachment to an opponent. Using some super-duper software, your opposing counsel is able to review the editing history to uncover an earlier version that gives new insights into your case's weaknesses. *Oops!*

Notice to sender

Here's the point: There's more to digital documents than meets the eye; it's just that you may have forgotten that (or never knew it). When opponents gain access to your client's confidences or your mental impressions, life gets complicated. Important concerns about confidentiality, attorney-client privilege and attorney work product come into play.

What's our guidance? In Indiana, it wasn't much until Jan. 1, 2005, when the Indiana Supreme Court put Rule of Professional Conduct 4.4(b) into play. Like its ABA Model Rule counterpart, it says: "A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender." That's all? Notify the sender? Yup, that's basically the beginning and end of the ethical obligation. Comment [2] to the rule says as much: "[W]hether a lawyer is required to take additional steps, such as returning the document is a matter of law beyond the

scope of these Rules, as is the question of whether the privileged status of a document has been waived." Comment [3] gives lawyers some authority for acting independently of their clients' wishes in the circumstances: "Whether a lawyer should return a document is ordinarily a matter of professional judgment reserved for the lawyer under Rules 1.2 and 1.4."

But what about this business of mining an opposing lawyer's digital documents for sensitive embedded data? Could that possibly be ethical? There's no clear guidance yet in Indiana. The scenarios at the beginning of this column illustrate that the documents themselves were not sent inadvertently. Yet embedded data was included as a part of the document, not intentionally, but through inadvertence or ignorance. Should Rule 4.4(b) apply or not?

Discovery is different

This ethical quandary is not to be confused with the somewhat related questions that arise when counsel produces a client's documentary evidence that was created and maintained in digital form pursuant to a discovery request. The Federal Rules of Civil Procedure were amended effective Dec. 1, 2006, to encourage counsel to negotiate the ground rules for e-discovery early and achieve agreements on how to handle discovered materials that might inadvertently include privileged embedded data. *See* Fed. R. Civ. P. 26(f). This situation is different because, in the world of e-discovery, digital documents are often sought to be produced in native format for the very

Donald R. Lundberg
Executive Secretary
Indiana Supreme Court
Disciplinary Commission
Indianapolis, Ind.

(continued on page 36)

reason that, absent the existence of a privilege, the embedded data is properly discoverable, and producing counsel should fully expect discovering counsel to mine the documents for embedded data. *See* Rule of Professional Conduct 3.4(a), which prohibits unlawfully altering, destroying, concealing evidentiary material or otherwise obstructing another party's access to it.

The same is not true for the myriad electronic communications that flow between lawyers as a case unfolds or a negotiation advances. Here, it is undoubtedly the case that sending counsel did not intend that opposing counsel would mine a document for confidential embedded data.

What others say

To date, a few ethics opinions address this evolving techno-ethical morass, most notably a recent opinion from the ABA Standing Committee on Legal Ethics and

Professional Responsibility. ABA Opinion 06-442. Before the ABA incorporated Model Rule 4.4(b) into its legal ethics code, this question was governed at the ABA level by ABA Opinion 92-368. That opinion (on inadvertently sent documents – not embedded data) said that the lawyer who receives a document known to be inadvertently sent has three duties: (1) refrain from examining it; (2) notify the sending lawyer; and (3) follow the sending lawyer's instructions.

With the advent of Rule 4.4(b), new Opinion 06-442 states that embedded data should be treated the same as any other inadvertently sent document under Rule 4.4(b). That is to say, there is no ethical restriction on the receiving lawyer mining a digital document for embedded data and making use of that data. The only ethical duty is to notify the sender upon discovering embedded data that reasonably appears to have been inadvertently

sent. On this latter point, the opinion declines to set a bright-line standard, suggesting that the duty to notify the other side may differ from case to case depending upon the specific facts. Presumably, the committee meant that the duty to notify hinges upon whether the embedded data would appear to a reasonable observer to have been inadvertently sent.

The ABA's position has supporters and detractors. Notably, in the support column, Maryland Opinion 2007-09, going even further than the ABA, concludes that Maryland lawyers have no ethical duty to let the other side know when a digital document contains privileged embedded data. Noted, though, that Maryland does not have an analog to Model Rule 4.4(b).

The New York State Bar Association has come out the other way, also in a state that does not have an analog to Model Rule 4.4(b). NYSBA Opinion 749 (2001) took the position that it was unethical to mine a digital document for embedded data. More recently, NYSBA Opinion 782 (2004) ratified and refined its position that a receiving lawyer should not exploit an inadvertent transmission of confidences contained in embedded data. The clear suggestion from New York is that its lawyers should not look for embedded data and upon nonetheless discovering it should follow the 1992 ABA protocol by not using it, informing the other side, and abiding by the other side's instructions.

Florida, which has an analog to Model Rule 4.4(b), has come out squarely against the new ABA position. In Ethics Opinion 06-02, Florida lawyers were instructed to avoid mining non-discovery documents from opponents for embedded data and upon discovering such notify opposing counsel.

Caveat scriptor

Where should Indiana lawyers come down? Let's start with a fundamental proposition: Lawyers are duty-bound to protect their client's confidences. Indiana Rule of Professional Conduct 1.6(a). In an age of ubiquitous digital communications between lawyers, it is quickly becoming less forgivable to include sensitive or confidential embedded data in communications sent to opponents. Protective measures can be taken. Readily available Metadata-scrubbing software should be employed before sending digital documents. If a document does not have to be edited by the receiver, converting a document to .pdf format will eliminate most embedded data. If the sending lawyer takes care of business, the other ethical quandaries disappear.

Unclean hands from data mining

Just as with misdirected faxes or mail, mistakes can be made. While data mining of discovery documents should be expected, it is rarely justifiable for lawyers to mine routine digital transmissions from opponents for privileged embedded data, just as it should be impermissible for opposing counsel to listen intently outside an opponent's mediation caucus room in hopes on hearing something useful or to catch a glimpse of another lawyer's trial notes on counsel table. And when obviously confidential data is inadvertently discovered, I don't buy the view that Rule 4.4(b) has no application because the host document was intentionally sent. Rule 4.4(b) says you let the sender know and fight over the consequences later.

Questions of law predominate

After the sender has been notified, what then? I agree with the ABA that now we are out of the ethics swamp and into the world of evidentiary privileges and waiver. The law of waiver due to inadvertent disclosure is quite complicated and largely beyond the scope of this column, but here's a teaser.

The cases on point fall along a spectrum running from "inadvertent disclosure is a *per se* privilege waiver" to "inadvertent disclosure is never waiver because it was not intended." A middle position uses a multi-factor analysis that was discussed in an excellent opinion by Judge David Hamilton in *Draus v. Healthtrust, Inc.*, 172 F.R.D. 384 (S.D. Ind. 1997). These factors are: "(1) the reasonableness of the precautions taken to avoid the inadvertent disclosure; (2) the time taken to rectify the error; (3) the scope of the discovery; (4) the extent of the disclosure; and (5) the 'overriding issue of fairness.'" *Id.* at 387 (citation omitted.) Applying

these factors, courts have not been very protective of lawyers who let privileged information slip. Even so, a lawyer who receives obviously privileged information from an opponent and reads it anyway, runs some risk of being compelled to return it and having the bell un-rung by being disqualified from the case.

Whatever the outcome of the privilege fight, the core ethical duty is to notify the sending lawyer that obviously privileged or otherwise confidential information has apparently been sent inadvertently. It is less clear whether receiving lawyers should mine non-discovery documents for embedded data in the first place in hopes of discovering privileged or confidential information. As indicated above, I think it's wrong.

The time has passed for lawyers to remain ignorant of the ethical implications of using modern communications technology. Whether a consensus will develop over the issues that arise when lawyers operate in this environment remains to be seen. ☺