NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 8, ISSUE 2: SPRING 2007

MINING FOR EMBEDDED DATA: IS IT ETHICAL TO TAKE INTENTIONAL ADVANTAGE OF OTHER PEOPLE'S FAILURES?

David Hricik[1]

Embedded data is information, including metadata, that accompanies many common word processing files, but which is ordinarily not seen on the screen. Unless a lawyer removes embedded data from a file before sending the file to opposing counsel, the embedded data accompanying the file could reveal confidential or privileged information. The authorities disagree on whether the transmission of embedded data is either "inadvertent" or "dishonest" in terms of the disciplinary rules. This Article contends that transmission of embedded data should be at least presumptively inadvertent and that it is dishonest for a lawyer to actively look for embedded data.

I. THE INEVITABILITY OF INADVERTENT TRANSMISSION

Lawyers transmit both paper and electronic documents to opposing counsel and third parties every day. Obviously, lawyers have an obligation to take reasonable care to not disclose information to an opposing or third party that is privileged, confidential, or subject to work-product protection.[2] Inadvertent disclosure of confidential information can harm the client by waiving any claim to the protected status of the information or by

[1] Associate Professor of Law, Mercer University School of Law, Macon, Georgia. The title is inspired by John Wesley Harding's song "Other People's Failure" from the compact disc John Wesley Harding's New Deal (Rhino 1996). I would like to thank the editors of North Carolina Journal of Law & Technology for inviting me to participate in their symposium and for their hospitality during the event, and to Wesley Stace for being such a good sport about the song titles.

[2] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (2003) ("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.").

simply letting the cat out of the bag, harming the client regardless of whether the information is admissible at trial.[3]

However, despite the exercise of reasonable care, lawyers have continued and will continue to inadvertently transmit confidential information[4] to an opposing or third party. Either they will fail to take appropriate technological safeguards,[5] or those safeguards will fail despite the lawyer's best efforts. Accidents will happen.[6]

That is why many lawyers have found themselves in the position of having to determine how to respond when they inadvertently received a document from opposing counsel.[7] Since perfection is unattainable, lawyers will continue to be put in this position notwithstanding the rise of technological "cures" to inadvertent transmission of embedded data.[8]

[3] *See In re* Sealed Case, 877 F.2d 976 (D.C. Cir. 1989) (holding that inadvertently disclosing privileged information waives the privilege); Georgetown Manor v. Ethan Allen Corp., 753 F. Supp. 936 (S.D. Fla. 1991) (holding that inadvertent disclosure can never waive privilege); Alldread v. City of Grenada, 988 F.2d 1425 (5th Cir. 1993) (holding that inadvertent disclosure can sometimes waive privilege).

[4] For simplicity, this Article refers to information that is protected against disclosure by rules governing confidentiality, work product, or other privilege law as "confidential information." It should be noted, however, that there are important differences not implicated by the discussion here that arise out of the status of the information. For instance, it may be that confidentiality is lost by inadvertent transmission, but the ability to object to the admissibility of the information at trial remains intact. *See, e.g.*, Purcell v. Dist. Att'y for Suffolk Dist., 676 N.E.2d 436 (Mass. 1997) (holding that certain information was no longer confidential, but was still privileged and so inadmissible at trial).

[5] Although there are a growing number of software fixes to the problems created by embedded data, nothing is foolproof. *See generally* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006) [hereinafter Op. 06-442].

[6] *See, e.g.*, Jones v. Eagle–North Hills Shopping Centre, L.P., No. 06-CIV-161-RAW, 2007 WL 184712 (E.D. Okla. 2007) (e-mail inadvertently sent by plaintiff's counsel to defense lawyer).

[7] *See generally* Andrew M. Perlman, *Untangling Ethics Theory from Attorney Conduct Rules: The Case of Inadvertent Disclosures*, 13 GEO. MASON L. REV. 767 (2006) (collecting and thoroughly discussing the issues concerning inadvertent transmission of confidential information).

[8] *See, e.g.*, Op. 06-442, *supra* note 5 (discussing various software "fixes").

Because of recent advancements in communication technology, more documents are exchanged today than ever before. This recent proliferation of both electronic communications and electronic documents has dramatically increased the frequency with which mistakes can happen.[9] Consequently, it is easier to make a mistake.[10] Now it only takes the click of a mouse—an accidental "reply to all," for example—to inadvertently transmit a privileged electronic file.[11]

In addition, unlike the paper they replace, electronic files that appear proper to send to opposing or third parties can contain "hidden" information that can, nonetheless, be confidential.[12] A file created in Microsoft Word, for example, when viewed on a screen by defense counsel, may simply show a plaintiff's settlement offer. However, this file might contain "hidden" comments between plaintiff's lawyer and client that reveal direct or inferential information about their settlement strategies or "bottom lines."[13] Unless specific steps are taken to reveal it, the "hidden" information is typically not visible when the document is

[9] Perlman, *supra* note 7, at 772–75 (describing sources of increase).

[10] *Id.*

[11] By way of anecdote, in the last case I helped try, we communicated frequently with opposing counsel by e-mail. A dispute developed as to whether opposing counsel were required to disclose the address of a potential witness to us. One lawyer on our side wrote an e-mail to one lawyer on their side asking them to do so. In response, we all received a reply, obviously intended only for their side, in which one of their lawyers in response to our lawyer's request told another of their lawyers to tell us "to go to hell." That e-mail became an exhibit at a hearing on a motion to compel identification of that witness. When our lead lawyer was pulling the e-mail out to use it, I heard one of their lawyers say to another in a whisper, "here it comes."

[12] For a thorough background as to why and how software like Microsoft Word and Corel WordPerfect create and store embedded data, see David Hricik, *I Can Tell When You're Telling Lies: Ethics and Embedded Confidential Information*, 30 J. LEGAL PROF. 79 (2006).

[13] Another anecdote: while speaking about this topic to small-firm and solo practitioners, one lawyer approached me during the break and explained that he had received a proposed contract from the opposing party which contained embedded data in the form of "comments" that revealed the other side's bottom lines, and even descriptions of negotiating strategies and other tactics.

printed or when the document is viewed in the creating word processing program.[14]

Ultimately, not only are electronic documents more frequently transmitted, they are more easily misdirected. In addition, they can contain confidential information that is not visible either in the printed document or in the document as typically viewed on the computer screen. This Article addresses the ethical obligations of lawyers who, outside the context of document production,[15] receive electronic files from opposing or third parties which contain embedded confidential information. It addresses a question that has split the bar: is it unethical to intentionally take steps to look "behind" the document to see the embedded data?

[14] *See* Hricik, *supra* note 12 (explaining the steps necessary to reveal embedded data). While embedded data often can be viewed with the program that created the particular file, specific steps must be taken to do so.

[15] It is important to emphasize that this Article is limited to inadvertent receipt outside the context of document production. Rules such as the new Federal Rules of Civil Procedure may replace or augment the issues of ethics discussed here if the issue is inadvertent production of documents during litigation. For example, amended Federal Rules of Civil Procedure 26(b)(5)(B) provides a process for "clawing back" a privileged document produced during discovery:

> If information is produced in discovery that is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved.

FED. R. CIV. P. 26(b)(5)(B).

II. THE ETHICS OF INTENTIONALLY TAKING ADVANTAGE OF OTHER PEOPLE'S FAILURES

"The first thing [some lawyers] often do when they get documents[—i.e., electronic files—]from the opposition is to look for metadata to see who drafted it or look for embedded versions of earlier drafts."[16] Most likely, the lawyer who looks for embedded data is hoping that the lawyer who sent it either failed to remove the information or failed in his attempt to do so. The bar associations are split on whether trying to uncover this hidden information is ethical. Some hold that taking active steps to view embedded data violates two ethical rules, while others hold it violates none.

Two issues arise in this context. First, is the inclusion of embedded confidential data in an intentionally transmitted file "inadvertent," requiring that the recipient notify the sender of the mistake as if the embedded data was a misdirected fax? Second, is it "dishonest" to take active steps to view embedded data?

A. *Is Embedded Confidential Information Inadvertently Sent?*

1. *The Law of Inadvertent Transmission*

It is important to survey the approach that courts and bar associations take to the typical form of inadvertent transmission—a misdirected fax or e-mail—in order to understand whether the same law applies to the receipt of embedded data. This section briefly describes that body of law.

The authorities have identified two forms of transmission that implicate the ethical rules. One occurs when a lawyer inadvertently includes an unintended person as a recipient of correspondence.[17] For example, this scenario occurs when counsel

[16] Jason Krause, *Guarding the Cyberfort*, 39 ARK. LAW. 25, 31 (2004) (bracketed material in original) (quoting Vincent Polley).

[17] The ABA mentioned inadvertent transmission of e-mail when analyzing waiver of privilege over a misdirected fax. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992), *withdrawn*, ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 05-437 (2005) [hereinafter Op. 92-368] ("[T]he availability of xerography and proliferation of facsimile machines and electronic mail make it technologically ever more likely that

sends a fax to opposing counsel that was intended for a client.[18] The second form, which is actually an unauthorized transmission, occurs when an unauthorized person intentionally transmits privileged information to an opposing party.[19] This latter form of transmission happens when, for example, disgruntled employees mail opposing counsel confidential documents that harm their employer.[20] Presumably, a file sent without authority will continue to be viewed under the "unauthorized" rubric and not as an instance of inadvertent transmission. Therefore, this Article focuses on the more prototypical form of inadvertent transmission.

Even before the rise of e-mail, this form of inadvertent transmission was so common that the American Bar Association (ABA) issued a formal opinion in 1992 addressing the obligations of lawyers who receive inadvertent transmissions. In ABA Formal Opinion 92-368,[21] the ABA concluded that lawyers who receive facially confidential or privileged materials should refrain from examining them, notify the sender, and follow the sender's instructions. Moreover, many individual jurisdictions have concluded that when a lawyer receives confidential information and the circumstances clearly indicate that the transmission was inadvertent, the recipient has an ethical duty to notify the transmitting lawyer of the mistake and, in some jurisdictions, follow the transmitter's instructions on how to proceed.[22]

through inadvertence, privileged or confidential materials will be produced to opposing counsel by no more than the pushing of the wrong speed dial number on a facsimile machine."); *accord* Fla. State Bar Ass'n. Comm. on Prof'l Ethics, Op. 93-3 (1994) [hereinafter Op. 93-3] ("Such an inadvertent disclosure might occur as part of a document production, a misdirected facsimile or electronic mail transmission, a 'switched envelope' mailing, or misunderstood distribution list instructions.").

[18] Op. 92-368, *supra* note 17; Op. 93-3, *supra* note 17.

[19] *See generally* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 94-382 (1994) [hereinafter Op. 94-382], *withdrawn*, ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-440 (2006) (collecting cases).

[20] *See id.*

[21] *See* Op. 92-368, *supra* note 17.

[22] *See* Perlman, *supra* note 7, at 783–85 (collecting authorities); *see generally* Douglas R. Richmond, *Key Issues in the Inadvertent Release and Receipt of Confidential Information*, 72 DEF. COUNS. J. 110 (2005); James Q. Walker,

Later, the ABA adopted a rule that specifically governs the obligations of lawyers who receive information inadvertently sent by another party. Model Rule 4.4(b) provides: "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."[23] A comment to the rule explains that a lawyer who knows or reasonably should know that a document was sent inadvertently should "promptly notify the sender in order to permit that person to take protective measures."[24] The comments also specifically state that the rule covers inadvertently sent e-mail.[25]

In some ways, Model Rule 4.4(b) is broader than Formal Opinion 92-368; it covers all inadvertent transmissions, not just those which involve confidential information. On the other hand, the obligation imposed is narrower. In contrast to Formal Opinion 92-368, the only obligation imposed by Rule 4.4(b) is notice; whether the lawyer should refrain from looking at the document and whether the lawyer must abide by the sender's instructions are matters not addressed by the Model Rules.[26]

Model Rule 4.4(b) has been adopted in roughly fifteen jurisdictions.[27] In addition, bar and judicial opinions in many jurisdictions continue to impose more demanding duties upon lawyers who receive inadvertently transmitted documents from another lawyer than those imposed by Rule 4.4(b).[28] The

Ethics and Electronic Media, 716 PRACTICING LAW INST., LITIG. 313, 334–36 (2004).

[23] MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2003) (emphasis added).

[24] *Id.* at cmt. 4.

[25] *Id.*

[26] *Id.*

[27] Perlman, *supra* note 7, at 783.

[28] *See id.* at 783–84; *see, e.g.*, N.Y. City Bar Ass'n Comm. on Prof'l & Jud. Ethics, Op. 2003–04 (2004) [hereinafter Op. 2003–04] (concluding that a lawyer who receives misdirected documents must, if it contains "confidences" or "secrets," advise the sender of the mistake, unless the lawyer has a good faith belief that a tribunal before which a dispute is pending will conclude confidentiality has been waived); N.Y. County L. Ass'n Ethics Comm., Op. 730 (2002) (concluding that a lawyer should assist in preserving the confidences of a sender of inadvertently privileged documents); Op. 92-368, *supra* note 17

requirements imposed upon lawyers by these bar opinions vary significantly,[29] however, and not every jurisdiction has adopted either an opinion or Model Rule 4.4(b) to address this issue.[30] Nonetheless, the authorities addressing the issue have imposed at least an obligation of notice on lawyers who receive information under circumstances where he or she knows, or should know, that the information is confidential and was inadvertently sent.[31]

2. *The Nature of Inadvertence*

Because the ethical obligations of lawyers depend on the presence of "inadvertence," it is important to be clear about what is "inadvertent" and what is "advertent" in this context. This traditionally clear dichotomy is challenged by electronic communication. Consider the lawyer who creates a file and sends it to the very lawyer to whom he meant to send it, but the file contains embedded confidential information that the sending lawyer did not know was going along with the file. Can the transmission of the embedded data be characterized as inadvertent when it is clear that the lawyer intended to transmit the file, but not to send the embedded data? Thus, the inadvertence associated with the embedded data is the converse of the fax situation: the recipient is intended but the content is not.

In the typical Model Rule 4.4(b) scenario, the receiving lawyer knows that the document was not intended for him, since it was probably addressed to another person or the document revealed strategies for litigation or settlement. It is not a great leap, under those circumstances, to conclude that the recipient knew or should have known that the information was inadvertently sent.

Can the same thing be said about embedded data? After all, intentionally sending a file with the embedded data makes the

(concluding that the recipient of misdirected communication should advise sender of the mistake and abide by its instructions).

[29] *See* Op. 2003–04, *supra* note 28 (discussing variations and disagreements on the duty).

[30] Perlman, *supra* note 7, at 781–83. Some state bar associations reject Model Rule 4.4(b). For example, in Md. Bar Ass'n Inc., Op. 2007-9 (2007), the Maryland Bar Association held that there is no obligation concerning misdirected documents because Maryland had not adopted Model Rule 4.4(b).

[31] Perlman, *supra* note 7, at 783–85.

transmission, to some extent, advertent. There was no mistake as to which file to send.

An analogous situation would be when a lawyer mails one document to opposing counsel, but unknowingly includes in the envelope another document that contains confidential information. No doubt, the lawyer intended to send one document. The courts and bar associations have had no difficulty in concluding that this does not mean that he intended to send both.[32] Thus, the unintentional inclusion of a confidential document is inadvertent notwithstanding its association with a document that was sent intentionally.

Arguably, the situation of embedded data may be different because there is only one document involved; the lawyer intended to transmit *the file* and *that file* contained the embedded data. Even so, can the transmission of confidential data in the file nonetheless be deemed to be inadvertent?

The authorities are split on the answer to this question.

3. *Existing Authority on Embedded Information and Inadvertent Transmission*

The New York Bar Association was the first to address this issue and took the position that inclusion of embedded confidential information may be inadvertent, even if it is included in an intentionally transmitted file.[33] New York Opinion 749 established a strong presumption of inadvertence, recognizing that, although the transmitting party intended to transmit the "visible" document, "absent an explicit direction to the contrary counsel plainly does not intend the lawyer to receive the 'hidden' material or information."[34] Thus, the New York State Bar concluded that lawyers who receive files with embedded data either know, or should know, that the embedded data was not sent advertently.

[32] *See, e.g.*, Pa. Eth., Op. 99-150 (1999) (concluding that "ministerial errors"—along the lines of putting the wrong document in an envelope with the intended one—have been deemed "inadvertent").

[33] N.Y. State Bar Ass'n Comm. on Prof'l Eth., Op. 749 (2001) [hereinafter Op. 749].

[34] *Id.*

More recently, an opinion from Florida confirmed this view.[35] It concluded that lawyers should "not try to obtain from metadata information relating to the representation of the sender's client that the recipient knows or should know is not intended for the recipient. *Any such metadata is to be considered by the receiving lawyer as confidential information which the sending lawyer did not intend to transmit.*"[36] Thus, the bar associations of Florida and New York have both concluded that, even if the document was transmitted intentionally, the embedded data was not.

These opinions seemed to make sense. However, in an August 2006 opinion,[37] the ABA rejected the proposition that embedded data is always unintentionally sent.[38] Although the ABA seemed to suggest that *some* embedded data could be deemed to be inadvertently sent, its analysis on this critical point is less than clear.[39]

The ABA first concluded that Model Rule 4.4(b) by its terms does not apply and, instead, characterized the rule as merely the "most closely applicable rule" because it "relates to a lawyer's receipt of inadvertently sent information."[40] Emphasizing its disagreement with the proposition that embedded data is never unintentionally sent, the ABA stated that, although Model Rule 4.4(b) might require the lawyer to notify the sender of the receipt of the information if it was sent inadvertently, "the Rules do not contain any specific prohibition against a lawyer's reviewing and using embedded information in electronic documents."[41] Further, the Committee noted that it "does not characterize the transmittal of metadata either as inadvertent or as advertent, but observes that the subject may be fact specific."[42] The Committee ultimately stated that whether a receiving lawyer

[35] Prof'l Ethics of the Fla. Bar, Op. 06-2 (2006).

[36] *Id.* (emphasis added).

[37] Op. 06-442, *supra* note 5.

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.* at n.7 (noting that no rule "addresses the duty of a recipient of advertently transmitted information").

knows or should know that embedded data was sent "inadvertently" in terms of Model Rule 4.4(b) was a question "outside the scope of this opinion."[43]

4. *Who got it right?*

Embracing the proposition that embedded data is not *always—or at least not presumptively*—included unintentionally is startling, and it opens the door for lawyers to review embedded data first and ask questions later. This is striking because it is hard to imagine a scenario where a lawyer would *intentionally* include confidential information in the form of embedded information. Thus, as two other bar associations realized, a lawyer at least *should know* that any embedded confidential information was sent inadvertently.

The ABA's determination that inadvertence of embedded data transmission depends on the facts in which transmission arises ignores reality and gives license to recipient lawyers to contend that such information was included advertently. The ABA's approach also cannot be harmonized with the opinion's own characterization of embedded data as well-known. If the existence of embedded data was well-known, the transmission of embedded confidential information would have to be inadvertent because no lawyer intentionally sends confidences to the opposition. Thus, even on the ABA's own premises, the only reasonable conclusion is the presumption that embedded data was sent inadvertently.

What is even more troubling about the ABA's opinion is its failure to acknowledge that opening a document in a word processing program generally will not reveal embedded data. It takes intentional steps beyond the double-clicking required to view a word processing file to view embedded data. As the New York Opinion emphasized: "[I]t is a deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer, that would lead to the disclosure of client confidences and secrets."[44] The ABA did not address the fact that only active steps by the recipient result in true receipt of the embedded data.[45] As a result,

[43] *Id.*

[44] Op. 749, *supra* note 33.

[45] Op. 06-442, *supra* note 5, (reasoning that "[e]ven if transmission of 'metadata' were to be regarded as inadvertent, Rule 4.4(b) is silent as to the

the ABA permits lawyers to intentionally take advantage of other people's failures.

B. *Is it Dishonest to Review Embedded Data?*

Model Rule 8.4(c) provides that it is "professional misconduct" for a lawyer to "engage in conduct involving dishonesty, fraud, deceit or misrepresentation."[46] Rule 8.4(c)'s "prohibition . . . is a broad one. It encompasses conduct toward clients, tribunals, parties, witnesses, opposing counsel, and everyone else, both within and outside the realm of the practice of law. It covers the act of failing to disclose, as well as affirmatively lying."[47]

This section analyzes whether it is dishonest, within the meaning of Model Rule 8.4(c), to view embedded confidential information. The authority, once again, splits on this question and even on whether the answer matters.

ethical propriety of the use of such information"). In other words, Rule 4.4(b) merely requires notification to the opposing party of its receipt, but does not address what, if anything, the lawyer must do next. The conclusion is: in jurisdictions with Rule 4.4(b) or its equivalent, a lawyer who receives inadvertent transmissions must notify the other side, but how to proceed from that point is a matter beyond the scope of the rules. Comment 3 to Model Rule 4.4(b) states:

> Some lawyers may choose to return a document unread, for example, when the lawyer learns before receiving the document that it was inadvertently sent to the wrong address. Where a lawyer is not required by applicable law to do so, the decision to voluntarily return such a document is a matter of professional judgment ordinarily reserved to the lawyer.

MODEL RULES OF PROF'L CONDUCT R. 4.4(b) cmt. 3 (2003).

[46] MODEL RULES OF PROF'L CONDUCT R. 8.4(c) (2003).

[47] ABA ANNOTATED MODEL RULES OF PROFESSIONAL CONDUCT 609 (5th ed. 2003) [hereinafter ABA ANNOTATED].

1. *Does it Matter if it's Dishonest?*

Model Rule 8.4(c) is often characterized as a "catch-all."[48] In other words, "[o]ften, the same behavior that violates subsection (c) also violates . . . other ethics rules."[49] The role of these catch-all provisions, as well as the need to avoid reading them too broadly, was succinctly explained by the American Law Institute:

> Modern lawyer codes contain one or more provisions (sometimes referred to as "catch-all" provisions) stating general grounds for discipline, such as engaging "in conduct involving dishonesty, fraud, deceit or misrepresentation" (ABA Model Rules of Prof'l Conduct, Rule 8.4(c) (1983)) . . . . Such provisions are written broadly both to cover a wide array of offensive lawyer conduct and to prevent attempted technical manipulation of a rule stated more narrowly. On the other hand, the breadth of such provisions creates the risk that a charge using only such language would fail to give fair warning of the nature of the charges to a lawyer respondent and that subjective and idiosyncratic considerations could influence a hearing panel or reviewing court in resolving a charge based only on it. . . . Tribunals accordingly should be circumspect in avoiding overbroad readings or resorting to standards other than those fairly encompassed within an applicable lawyer code.
>
> No lawyer conduct that is made permissible or discretionary under an applicable, specific lawyer-code provision constitutes a violation of a more general provision so long as the lawyer complied with the specific rule . . . .[50]

Thus, although Rule 8.4(c) is intended to catch conduct that falls outside the technical reading of the other rules, it should not be interpreted in a manner that either results in a failure of notice or punishes what another rule permits.

As noted below, other bar associations have applied this catch-all to the question of whether it is dishonest to review embedded data. However, the ABA reasoned that because Model Rule 4.4(b) addresses inadvertent transmission, the issue of dishonesty was irrelevant: "[T]he recent addition of Rule 4.4(b) identifying the sole requirement of providing notice to the sender

[48] *See, e.g.*, *In re* Alcorn, 41 P.3d 600, 611 (Ariz. 2002) (referring to Arizona's equivalent of Rule 8.4(c) as a "catch-all").

[49] ABA ANNOTATED, *supra* note 47, at 609.

[50] RESTATEMENT (THIRD) LAW GOVERNING LAWYERS § 5 cmt. c (2000).

of the receipt of inadvertently sent information, [is] evidence of the intention to set no other specific restrictions on the receiving lawyer's conduct found in other Rules."[51] In support of its conclusion that Model Rule 8.4(c) was no longer intended to play its gap-filling role under these circumstances, the ABA pointed only to the following reporter's explanation of why Model Rule 4.4(b) was added to the Model Rules:

> Numerous inquiries have been directed to ethics committees regarding the proper course of conduct for a lawyer who receives a fax or other document from opposing counsel that was not intended for the receiving lawyer. ABA Standing Committee on Ethics and Professional Responsibility Formal Opinion 92-368 advised that the receiving lawyer is obligated to refrain from examining the materials, to notify the sending lawyer and to abide by that lawyer's instructions. That opinion has been criticized, in part because there is no provision of the Model Rules directly on point. The Commission decided that *this Rule should require only that the lawyer notify the sender when the lawyer knows or reasonably should know that material was inadvertently sent*, thus permitting the sending lawyer to take whatever steps might be necessary or available to protect the interests of the sending lawyer's client.[52]

By relying on this unadopted reporter's note that fails to mention Rule 8.4(c), the ABA's opinion ignores a key distinction between the problem of embedded data and other instances of inadvertent transmission. While the reporter's note does emphasize that the lawyer's only obligation upon receiving information inadvertently is to notify the recipient, it fails to address whether it is dishonest for a lawyer to *search for it* in the first place. Rather, the note merely states that his only obligation under the Model Rules is to notify the sender if he finds it. Thus, the ABA's conclusion that the dishonesty of the conduct is irrelevant places more weight on the reporter's note than it can support.

Moreover, the reporter's note does not necessarily make the dishonesty of *looking at* the embedded data irrelevant, nor does

[51] Op. 06-442, *supra* note 5.

[52] Am. Bar Ass'n Center for Prof'l Responsibility, Model Rule 4.4 Reporter's Explanation of Changes, http://www.abanet.org/cpr/e2k/e2k-rule44rem.html [hereinafter Reporter's Explanation] (emphasis added) (last visited Mar. 29, 2007).

any authority cited in the ABA's opinion require the conclusion that Model Rule 8.4(c) is irrelevant. Reading Model Rule 8.4(c) to prohibit examining embedded data does not conflict with Model Rule 4.4(b), because nothing in Model Rule 4.4(b) necessarily permits a lawyer to look at embedded data. Additionally, Rule 4.4(b), as interpreted by the ABA, requires a lawyer who *knows* embedded data has been sent inadvertently to notify the transmitting lawyer, which suggests that looking may be unethical.

The question then becomes, is it dishonest to look?

2. *Is It "Dishonest" to View Embedded Data?*

Recall that, normally, embedded confidential information is invisible; that is why it is accidentally included. Thus, for a recipient to view embedded data, he typically must take active, deliberate steps to reveal the information.

Not surprisingly, bar associations have concluded that taking active steps to look at confidential information is dishonest. The New York bar association recognized that it smacked of dishonesty for a lawyer to "intentional[ly] use . . . computer technology to surreptitiously obtain privileged or otherwise confidential information from an opposing party."[53]

The ABA disagrees on this issue, as well. After finding the issue of dishonesty irrelevant, the ABA reasoned that it was not dishonest for a lawyer to take active steps to review embedded data that had been inadvertently sent by another lawyer.[54] Its conclusory explanation states twice only that "the Committee does not share" the view of other bar associations that intentionally looking to see if a lawyer included client confidences was dishonest.[55]

Because of the factual premises of the ABA's argument, the opinion's conclusion is untenable. The ABA opinion assumes that it is well-known that files contain embedded data and that embedded data comes in an understandable form.[56] These

[53] Op. 749, *supra* note 33.

[54] Op. 06-442, *supra* note 5.

[55] *Id.*

[56] *Id.*

assumptions[57] do not change the fact that sensitive embedded data will be included in a transmitted document only when the lawyer sending it makes a mistake, i.e., an inadvertent transmission. No lawyer intentionally transmits confidential information to an opponent. Indeed, the fact of common *inadvertent* transmission is what led the ABA to adopt Model Rule 4.4(b) in the first place.[58] Yet, the ABA opinion reasoned that it is not dishonest for the receiving lawyer to *actively take steps* to uncover confidential information that—under the opinion's assumptions—almost by definition had to be inadvertently included.

Finally, the assumptions that embedded data is well-known and understood crumble in the face of continued reports of inadvertently transmitted embedded data. The only study located found that, rather than being well-known, in as late as 2004, only 43% of respondents were aware that embedded data even existed.[59] Reflecting that fact, major law firms have posted "filed versions" of complaints on the Internet which contained embedded data that revealed prior revisions, comments, and other embedded data.[60] Corporations, governments, individual lawyers, and others have done the same.[61] Patches offering fixes and warning about embedded data were released only in late 2006,[62] at virtually the same time the ABA issued its opinion stating that everyone knew

[57] In my opinion, the ABA's assumption is clearly wrong. I have lectured about embedded data to several hundred lawyers in states from Rhode Island to Florida to Texas to California. The vast majority had no clue what metadata was before I began to speak.

[58] Reporter's Explanation, *supra* note 52 (explaining that "numerous inquiries" about misdirected documents had led to the adoption of Rule 4.4(b)).

[59] Stephen Shankland, *Hidden Text Shows SCO Prepped Lawsuit Against BofA*, NEWS.COM, Mar. 4, 2004, http://news.com.com/2102-7344_3-5170073.html?tag=st.util.print.

[60] *Id.*

[61] *See* Tom Mighell & Dennis Kennedy, *Staying on Track with Track Changes*, ABANET.ORG, Mar. 2007, http://www.abanet.org/lpm/lpt/articles/slc03071.shtml (last visited Apr. 11, 2007).

[62] For example, Corel's patch—which fixed a bug in its earlier "metadata fix" that allowed comments to remain with a document even after they had been "removed"—was made available in July 2007. *See* WordPerfect Office X3 Service Pack 1 (July 26, 2006), http://www.corel.com/content/wpo/WPOSP1_Patch_Readme.htm (last visited Apr. 15, 2007).

and understood about embedded data. Given the realities, the ABA's conclusion that embedded data is not sent inadvertently, or is not presumed to have been sent inadvertently, is inexplicable.

The notion that a lawyer should be permitted to look for inadvertently transmitted embedded data and, thereby, intentionally take advantage of the accidental failure of a colleague to understand the inner workings of software is startling. The characterization of the intentional act of taking advantage of those mistakes as anything less than dishonest is disappointing.

III. CONCLUSION

We have not heard the last word on this issue.

After lecturing about embedded data in front of hundreds of lawyers across the country, my impression is that lawyers in large law firms or more sophisticated law firms are aware of these issues. However, in my experience, the bulk of lawyers—those in small firms and those who practice alone—are almost uniformly and completely unaware of the existence of embedded data. Thus, in some measure, the ABA's opinion provides protection to lawyers in large firms because it allows them to look for embedded data that they both know are there and know should not be there.

In my view, until it is clear that lawyers beyond those in the largest or most sophisticated firms know about embedded data, the courts and bar associations should hold that the transmission of embedded data is either per se or presumptively inadvertent transmissions. Further, lawyers should be required to refrain from looking for embedded data and to notify the other side when they learn that it has been received. In other words, courts should not let lawyers intentionally take advantage of other people's failures.