I CAN TELL WHEN YOU’RE TELLING LIES: ETHICS AND EMBEDDED CONFIDENTIAL INFORMATION

David Hricik

I. INTRODUCTION

The risk of inadvertently transmitting what a lawyer knows is confidential information to an opposing or third party has always existed. Not too long ago, the primary risk was that a letter intended for a client would instead be mailed or faxed to opposing counsel.1 For example, a lawyer might have made handwritten comments on a contract proposal drafted by the other side, and, though intending to forward the document to the client for review, may have inadvertently mailed or faxed it to opposing counsel.

The digital age has increased the opportunity for and changed the means by which misdirection occurs, but in substance the circumstances leading to misdirection remain the same. Instead of misaddressing envelopes, today lawyers and their staff may inadvertently send e-mail intended for a client to opposing counsel or a third party or accidentally forward to opposing counsel an e-mail received from a client.2

Despite these changes in form, the ethical principles that apply to these typical forms of digital misdirection are no different than those that apply in the analog world. The lawyer who inadvertently discloses a client’s confidences can violate ethical duties,3 and at the same time a lawyer who re-

---

receives privileged information not intended for him may be ethically required to return the information unread, or take other steps.\(^4\)

The focus of this Article is a slightly more interesting and as yet largely unanalyzed form of misdirection: the intentional transmission of a computer file that carries with it "invisible"\(^5\) confidential information. The presence of this "invisible" information presents new twists on this old ethical problem, and the invisible information can be as important—if not more so—as the visible content of the file. The invisible information that accompanies some files "can reveal a cache of information, including the names of everyone who has worked on or seen a specific document, text and comments that have been deleted and different drafts of the document."\(^6\)

The question of lawyer's responsibilities concerning the transmission and receipt of this information presents issues distinct from both the traditional misdirected letter and its modern counterpart, the misdirected e-mail, from the perspective of both the sender and recipient. This Article addresses two distinct issues that metadata and similar forms of electronic data present. (Collectively, metadata and similar forms of data are referred to as "embedded data").

First, it analyzes whether lawyers have an obligation to be aware of embedded data and, as a consequence, to remove it from documents where it is ethically necessary and proper to do so. Did Macrosoft's lawyers, for example, violate duties to their client by unknowingly sending embedded data along with the text of the contract to opposing counsel? If there is such an obligation, what must lawyers do to comply with it?

Second, if a lawyer receives a file that contains embedded data that reveals confidential or privileged information of an opposing party, do the same obligations apply as when a lawyer receives a document in a misaddressed envelope?\(^7\) For example, did the lawyer who examined Macrosoft's internal commentary about the contract's terms violate any ethical obligations? If so, what does a lawyer who receives an electronic file do?

This Article addresses these issues\(^8\) but begins with an overview of the various common forms of embedded data before turning to the ethical issues that it creates.

---

5. See infra note 6 and accompanying text (The information is not really invisible. It can be viewed, but only if certain steps are taken. Those steps, however, do not require special software; the "invisible" information may be examined by using the program that created the file). In addition, programs specifically designed to view embedded data also exist.
7. See infra notes 71-98 and accompanying text.
8. Embedded data presents a third issue of competency for litigators during discovery in disputes where there exist relevant electronically-created documents. Just as the fax band may show that the opposing party is lying when he claims not to have received a document, so too embedded data may be highly relevant to a party's claim or defense in litigation. Therefore, is there an ethical obligation to seek out and discover the original files of critical documents in a case, so as to examine the embedded data for pertinent information? If, for example, a dispute arose over that contract with Macrosoft, do the litigators have an ethical obligation to seek out discovery of the actual electronic files, since the embedded
II. WHAT IS EMBEDDED DATA?

A. Overview of Embedded Data and Its Purposes

There are two somewhat similar forms of information that accompany electronic files: metadata and other information that is stored, and thus transmitted along, with electronic files.9

First, metadata is “data about data.”10 Although it sounds quite modern, one form of metadata is no doubt familiar to every lawyer: the fax band on a document received by facsimile. Typically, it shows the time and date the document was received, the number from which the fax originated, and the number of pages sent.11 A fax band is metadata, since it is data about data. The factual data it contains can be used in various ways. For example, it can be used to show that a party who claims it did not receive a document did receive it on a certain date.

Metadata pervades the digital world in which we live. Electronic files created by many common programs create metadata—hidden fax bands, and more—that is generally saved along with the visible text of the document. Oversimplifying it, “invisible fax bands” accompany files created by many modern computer programs. Metadata is embedded with the file and goes anywhere the file goes unless it is removed by the file’s creator prior to transmission. Any time the file is transmitted to another person, the fax bands go along with the file. But, rather than simply detailing the time and date the file was prepared, as would a true fax band, metadata often reveals much more.12

---


10. Often the two types are lumped into “metadata.” E.g., James Q. Walker, Ethics and Electronic Media, 716 PLL/LIT 313, 328 (2004); Carole Levitt & Mark Rosch, Making Metadata Control Part of a Firm’s Risk Management, 28 L.A. LAW. 40, 40 (2005). I prefer to separate out what is truly metadata—data reflecting when or who edited a document, for example—from other information that can be embedded in data files, such as prior revisions and undo histories. Treating the two as the same risks conflating the issue of whether confidentiality or privilege is likely to be conveyed by the transmission of files with embedded data. See infra notes 10-16 and accompanying text.

11. See infra note 12 and accompanying text for an example.

12. See infra notes 19-37 and accompanying text.
Electronic files are often accompanied by a similar, but distinct, form of information. In addition to metadata, many software programs permit authors to "[t]rack [c]hanges" to the text, to save "multiple undoes" in case the author later decides to "undo" revisions made previously, and to even overlay hidden comments into the text. This other information is also embedded with the file and accompanies the file unless removed prior to transmission.

An ostensibly true story demonstrates the potential risks of exchanging files with embedded data. Recently, a lawyer approached me after I had given a presentation about metadata and told me the following story. He had been negotiating a contract against a well-known software maker, whom we'll call "Macrosoft." During negotiations, the lawyers for each side used Microsoft Word to propose revisions to the contract, using its "track changes" feature to allow the recipient to see the specific changes each lawyer had made. They would e-mail the file with embedded data back and forth to each other between rounds of revisions. When the lawyer received one draft of the contract from Macrosoft's lawyers, he made a few mouse clicks and was easily able to reveal—without using anything but Microsoft Word—various "hidden" embedded data. As a result, he was able to read all of the internal comments that the sending lawyer had received from Macrosoft's business people concerning the terms of the contract, negotiating positions, and bottom-lines.

The receiving lawyer learned Macrosoft's critical bargaining information by clicking a button. He was able to see not only metadata showing who had revised the document, but also internal private comments that lawyers and business people on the other side had made. Thus, had a Macrosoft lawyer insisted during negotiations that the noncompetition clause was extremely important to Macrosoft, the lawyer I spoke to could use the internal comments where Macrosoft personnel had discussed the issue amongst themselves to tell if this were true, or if it was simply a negotiating ruse. He could tell when they were telling lies.

With that background, it is important to clarify the purpose of embedded data—it is there for a reason—before turning to specific examples of where embedded data can be found in the programs commonly used by lawyers today.
Embedded data is not created to cause the unintended exchange of confidential information. Although the form taken by embedded data varies among programs, the primary function of embedded data is utilitarian: it is designed to help users of software revise, organize, and access electronically-created files.\textsuperscript{17} Typical metadata includes, for example, the person who authored the document and its location (drive, folder). In addition, other embedded data can include records of past revisions. A secretary can, as a result, examine the changes that have been made to a file and compare them visually to any hand-written revisions to ensure that they have, in fact, been made. Thus, embedded data is useful.\textsuperscript{18}

\textbf{B. Specific Examples of Metadata}

This section provides some simple examples of embedded data to illustrate the kind and quality of information that these files can convey. Note that some of the particular illustrations and examples in each section will vary depending on the version of the software used.

\textit{1. Microsoft Word}

In my experience, lawyers commonly use Microsoft Word and commonly e-mail documents created by Microsoft Word to clients, third parties, and opposing counsel. It has rightly been called the “ubiquitous” software program.\textsuperscript{19} Embedded data is, unfortunately, ubiquitous in Word.

Metadata can be found by looking in different menu items in Microsoft Word.\textsuperscript{20} A key location is in the “Properties” item, located in the “File” menu. The “Properties” for a particular document can reveal the author, creation dates, and other information. For example, this particular article (as of about halfway through the writing process), contains the information under File/Properties as shown in Figure 1.

\begin{itemize}
\item\textsuperscript{17} See generally Brian D. Zall, \textit{Metadata: Hidden Information in Microsoft Word Documents and Its Ethical Implications}, 33 Colo. L.W., Oct. 2004, at 53.
\item\textsuperscript{18} See generally Hoenig, \textit{supra} note 10. “Word has built-in tools to facilitate collaboration among members of a team.” \textit{Id.} at 51.
\item\textsuperscript{19} Andrew Beckerman-Rodau, \textit{Ethical Risks from the Use of Technology}, 31 Rutgers Computer & Tech. L.J. 1, 32 (2004); see also Zall, \textit{supra} note 17, at 53-54 (describing legal profession’s adoption of Microsoft Word).
\item\textsuperscript{20} Interestingly, most metadata is stored in the last space of a Word document. If, for example, you copy all of a Word document except its last space (which will appear to be blank) and then paste that material into a new Word document, the prior metadata will not follow along. For a more technical discussion of how metadata is embedded in a Word document, see Zall, \textit{supra} note 17, at 54.
\end{itemize}
The metadata on just that single screen\textsuperscript{21} reveals the fact that I began to write this Article in August, and was still working on it in October, 2005. It also reveals that, as of the time I viewed that screen, it was the 44th revision (meaning I had opened and closed this document 44 times) and I had edited it for 205 minutes.\textsuperscript{22} If this document had been transmitted to a client, the client could have some insight into whether I had worked on it for as long as I said in my fee statement. If it were a report I had prepared as an expert witness, opposing counsel could discern how long I had worked on the report. If it were a brief that I had prepared as an undisclosed coun-

\begin{figure}
\centering
\includegraphics[width=\textwidth]{metadata.png}
\caption{Figure 1}
\end{figure}

\textsuperscript{21} I have only shown the screen for one of the five tabs: Each selection shows different information. Word generates much of this metadata automatically. The General selection shows the date and time the document was created (and modified and accessed), the size of the document, and the location of the document. The Summary selection shows the title of the document, the author's name, and the author's company, among other things. Users can also manually add comments about the document into fields under the Summary tab. Under the Statistics tab, anyone with access to the document can find the amount of time spent editing it, the name of the person who last saved it, the number of revisions, the date it was printed, and word count information. The Custom selection shows other documentation, such as the typist's name, the names of people the document was forwarded to, and the name of the client.

\textsuperscript{22} To be clear, the file could simply have been open on the screen for 205 minutes; the amount of time indicated does not necessarily mean that I was working on the file for all of those 205 minutes. It could simply have been open while I was teaching class, for example. Conversely, I could have been working on a hard copy for several more hours.
sel, and then counsel of record had forwarded the document, my identity would be revealed. Metadata matters.

More troubling than metadata is the other data that can accompany a Word file. Foremost, “Track Changes” is a feature that creates a record of every change made to a file. Its many uses include lawyers who exchange drafts of contracts, as mentioned in the introduction, can turn on track changes so that it is easy to spot revisions made to a proposed contract during negotiations; word processing personnel may turn on track changes so that they can review and ensure that they have made each handwritten edit desired by a lawyer; a co-author can turn on track changes to monitor edits; and so on.

The problem is that the author of the document may not know that “Track Changes” has been turned on, and the typical view on the screen of a Word document does not reveal the tracked changes. The changes will be “invisible.” For example, I wrote this paragraph, and then went back and turned on track changes. What you are reading now is the way the paragraph looked when I was finished editing it. Figure 2 shows what it looked like on October 23, 2005, with “Track Changes” turned on.

![Figure 2]

If I were to transmit the file that contains this Article to someone, he could easily reveal the changes and see the revisions to this document. If this were a contract, that could reveal to an opposing party revisions I had made to key terms of the proposed contract.

23. The kind and amount of information stored in the “Properties” file can be customized. To see whether your version has been customized, click on the “Custom” tab at the top of the “Properties” dialog box.

24. There are a number of other sources of metadata. For example, other tabs in the “Properties” pop-up box will show where the file was stored on my hard drive and other information.

25. See generally James Veach, Commutation Agreements: Drafting a Clear and Comprehensive Contract, 879 PULCOMMERCIAL LAW PRACTICE COURSE HANDBOOK SERIES 467 (2003) (explaining that track changes can be used in the drafting process to create better documents).

26. In order to turn on track changes, go to the “Tools” menu and to “Track Changes.” In order to see whether an open document contains tracked changes, turn on track changes, and then ensure that you are viewing the “Final Showing Markup.”

27. See Zall, supra note 17, at 55-56 (collecting hypotheticals on how metadata could harm clients and lawyers when exchanged with opposing counsel).
Another form of embedded Word data is created by the use of “Fast Saves.” If “Fast Saves” is enabled, then “deleted information remains hidden within the document.” Opposing counsel who receives a file that has been created with “fast saves” enabled can easily open the document and see all revisions.

Another form of embedded data that can accompany Word documents is “Comments.” Comments are incredibly useful for collaborative preparation of documents. For example, I am working with a colleague on a book on statutory interpretation. Each of us can make a comment to the other to explain the reason for a suggested a revision, inclusion of a certain concept, or the need for further clarification on some portion of the book. Those comments are embedded with the file and accompany it whenever we exchange the file. Figure 3 is a screen shot of a few lines from a chapter opened in Word with “View” set to “Showing Final Markup.” Notice also that the “Track Changes” information is displayed:

![Figure 3](image)

Moving up the continuum, a judge might use legislative history to confirm the meaning of the text. Should that be permitted or required? On the most conservative end of the continuum.

A final example is “Versions.” If “Versions” is enabled, then embedded with the file are all prior versions of the document. Each time it is saved, a new version is created and saved. Thus, once again if the file is transmitted to opposing counsel, she can view every prior version of the document.

---

28. This is done by selecting “Save As” from the “File” menu, then selecting “Tools,” and then “Save Options.” One option is “Allow Fast Saves.” Fast Saves is “very useful in the event of hardware failure because it reduces the chance of losing changes to a document.” Toby Brown, Special Handling: How Paper and Electronic Files Differ, 21 GPSOLO Sept. 2004, at 23. See also Hoenig, supra note 10, at 52 (explaining that while “Fast Saves” “makes saving a document faster . . . the time saving results . . . from the fact that text that has been deleted while editing the document is not actually deleted from the electronic file that produces the document.”).


30. Id. at 22-23.

31. See Zall, supra note 17, at 54-55. Various document management programs may impact this function. A lawyer in a firm using document management software should consult his IT department.
All of these features are useful to lawyers, their secretaries and their IT (information technology) staff. Lawyers need to be aware of the fact that these tools embed data with the file. Further, they also need to recognize that their staff may enable certain features without the lawyer’s knowledge.\footnote{Model Rule 5.3(b) requires lawyers with direct supervisory authority over a nonlawyer to “make reasonable efforts to ensure that the person’s conduct is compatible with the professional obligations of the lawyer.” The lawyer can, under some circumstances, be responsible for the nonlawyer’s conduct. \textit{See Model Rules of Prof’l Conduct R. 5.3} (2004).} For example, a good secretary may enable “Track Changes” so that he can double-check that all hand-written changes have been made. If the lawyer is unaware of the enablement of these features, and if the secretary doesn’t appreciate the problems created by transmitting the file with track changes still embedded, then disaster can strike.

2. Other Microsoft Programs

Like Word, other Microsoft products contain embedded data. For example, PowerPoint contains a “Properties” file. I downloaded from the Internet a blank “Jeopardy” file and the Properties from it reveals metadata shown in Figure 4.

![Figure 4](image)

In addition, “Speaker’s Notes” are a part of PowerPoint files. Speaker’s Notes are text that is not visible when a presentation is projected but which are visible to the speaker or can be printed out. They accompany the file when transferred unless removed beforehand.
3. Corel WordPerfect

Not only Microsoft products contain embedded data. Corel WordPerfect contains a “Properties” file that is somewhat less descriptive than Microsoft’s. Less information is, in the default mode, embedded in the “Properties” file than in Word. However, as in Word, this feature can be customized to include a variety of information, such as who received blind copies of the document. Disclosing to the other side who received blind copies of a document obviously defeats the purpose of sending blind copies.

In addition, WordPerfect contains a “Multiple Undoes” feature. When “Multiple Undoes” is enabled, the file is accompanied by embedded data that allows the recipient to “Undo” a large number of revisions to the document. The recipient might, for example, be able to “Undo” changes to a proposed settlement agreement to see how much the plaintiff’s opening offer was, and compare that to the amount actually mentioned in the first draft.

4. Adobe Acrobat

As noted above, many contend that one way to avoid transmitting embedded data is by converting the file into portable document format (“.pdf”). This is only partly true: a Word document saved into .pdf format will no longer carry with it the data embedded by the Word program. However, there are several caveats.

First, if the document is converted into .pdf format in the “View Final With Markup” setting, then the resulting .pdf document will show the comments and changes. Second, the document will still contain metadata: however, it will be the metadata created by Adobe Acrobat, not Word.

Even Adobe .pdf documents have embedded data, though less so than Word or WordPerfect. For example, I converted a later version of this Article into a .pdf file, and Figure 5 represents the metadata that accompanied it. There is clearly less metadata, but nonetheless the author, the time of creation, and the time of modification are visible.

Others have suggested that converting the file to “rich text format” (“.rtf”) eliminates embedded data. This is true only in part: the information in “Properties” will be deleted and will reflect only the information pertaining to the file after it was converted to .rtf; however, if the original

---

33. In WordPerfect, “Properties” is located on the File menu.
34. While in the “Properties” dialog box, select “Set Up” to view the possible customized features.
35. Generally, this means “Printing” the document to Adobe distiller.
37. To view this embedded data, go to the “File” menu, then to “Document Properties.”
38. Metadata can be viewed under “File” and then “Document Properties.”
39. See, e.g., Krause, supra note 6, at 26 ("Microsoft Word users can easily strip out much of a document’s metadata by saving it in the Rich Text Format, or .rtf"); Levitt & Rosch, supra note 9, at 40.
document had been created with “Track Changes” on, the resulting rich text document will continue to reveal tracked changes. Converting to .rtf is not a thorough solution.

Given the ubiquity of embedded data, what must lawyers who send it, or receive it, do?

III. THE ETHICS OF EMBEDDED CONFIDENTIAL INFORMATION

This section analyzes the ethical principles implicated by the creation and transmission of embedded confidential information.

A. The Duty to Avoid Disclosing Embedded Confidential Information

A lawyer representing a client must use reasonable care to avoid inadvertent disclosure of confidential information.40 Thus, two issues are presented: whether embedded data is “confidential information” and whether it violates a duty of care to transmit embedded data.

With respect to the issue of whether embedded data is “confidential information,” it is important at the outset to emphasize the distinction between the duty of confidentiality and the attorney-client privilege. The attorney-

40. See Model Rules of Prof'L Conduct R. 1.6 (2004).
client privilege is solely a rule of admissibility at trial,41 while the duty of confidentiality has nothing to do with trial admissibility.42 The duty of confidentiality can be implicated when that of privilege is not because "confidences" include, but are not limited to, "privileged" information.43 Therefore, the appropriate question with respect to the transmitting lawyer's duty of care is not whether embedded data is privileged, but whether it is "confidential."

The scope of the duty of confidentiality is broad,44 covering any information "relating to the representation of a client."45 The definition of confidential information clearly includes, but is not limited to, privileged information.46 Beyond that, it also requires protection of information which itself is not confidential but which could lead to disclosure of confidential information: "This prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person."47

For these reasons, it is clear that lawyers have an obligation to protect all information relating to the representation of a client.48 Obviously, they cannot intentionally disclose confidential information. Thus, a lawyer who knows of the presence of embedded data that consists of "confidential information" must remove it. For example, where data consist of track changes that reveal prior substantive revisions suggested by a client, the lawyer should avoid transmitting the document without first removing the embedded data, which likely constitute privileged information. Similarly, where the "Properties" in a document could reveal protected information—such as the fact that the document was authored by undisclosed co-counsel—the embedded data should be removed.49 A lawyer who transmits a document knowing that it contains embedded client confidences violates the duty of confidentiality.

41. See Purcell v. Dist. Attorney for Suffolk County, 676 N.E.2d 436 (Mass. 1997) (holding that information which was subject to disclosure as "not confidential" was still privileged).
42. See MODEL RULES OF PROF'L CONDUCT R. 1.6 (2004).
43. Id.
44. Id.
45. Id.
46. "The confidentiality rule... applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source." MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 3 (2004).
47. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 4 (2004).
48. Id.
49. It is extremely doubtful that all embedded data is a "client confidence." For example, the properties file shown from the .pdf version of this Article merely discloses the time and the fact that I wrote the document. It stretches the boundaries of "confidential" to deem those items confidential in most imaginable circumstances. See also Boenig, supra note 10, at 51 (noting that the .pdf file will "identify the user who prepared the document and the path to where the document is stored. This metadata, however, should very rarely be a problem."). Suppose, however, that the path reveals the name of an undisclosed principal who is interested in acquiring property without its identity being disclosed; even this minimal amount of embedded data could in some circumstances constitute confidential information.
The duty of confidentiality is not limited to intentional disclosure. In addition to having an obligation not to knowingly reveal confidential information, lawyers also have a duty to avoid inadvertent disclosure of confidential information. The fact that reasonable steps are required raises the question of whether a lawyer violates the duty of care by not discovering the complete nature of the file transmitted.

Do lawyers violate the duty of confidentiality if they knowingly transmit a document but are ignorant of the embedded confidential information? There are several ways this could occur, each of which requires different analysis.

First, the lawyer could have been aware of the presence of embedded data, and taken reasonable efforts to remove it, but nonetheless failed because of technological or user-related failures. It may be, for example, that a lawyer thought she removed the comments from a document, but had failed to "View" it in a way that would reveal the still-present comments. Similarly, the lawyer may have been aware that the program created embedded data but believed that the functionalities that create such data had been disabled.

It is easy to make mistakes even when exercising reasonable care and it seems that even experts disagree on whether particular approaches avoid disclosure of all embedded data. For these reasons, it is doubtful that a lawyer who either takes reasonable steps to remove metadata or who avoids creating it in the first place violates the standard of care or the duty of confidentiality. Obviously, this is a fact-intensive inquiry, but lawyers are not required to meet an unattainable standard.

Second, the lawyer could have created a file not knowing that it contained embedded data because the lawyer was unaware that the software created such data. Whether those circumstances violate the duty of confidentiality turns on the question of whether, at the time the document was created, a lawyer "should have known" of embedded data.

Clearly, lawyers have an obligation to take reasonable care to protect client confidences, a duty which includes an obligation to "stay abreast of technological advances and the potential risks." While some authors have essentially argued that "everyone knows" about embedded data, and so lawyers "should know" about it, in my own experience the opposite is true. In speaking about this issue to nearly 1,000 lawyers, it was apparent that the

---

50. MODEL RULES OF PROF'L CONDUCT R. 1.6 (2004).
51. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 16 (2004) ("A lawyer must act competently to safeguard information relating to the representation of a client 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.").
52. As noted above, for example, some say that converting a document to .pdf format removes all metadata, when in fact as shown here it simply replaces it with a different, lessened amount of metadata. See supra notes 35 to 39 and accompanying text.
53. N.Y. St. Bar Ass’n Comm. on Prof’l Ethics Op. No. 782 (Dec. 8, 2004). See Zall, supra note 17, at 56 (reasoning that attorneys must “exercise reasonable care by familiarizing themselves with the attendant risks associated with metadata and taking affirmative steps to eliminate the risks”).
vast majority had never heard of embedded data, let alone how to avoid creating it or how to remove it. Confirming my less-than-scientific poll, documents routinely show up on the web which contain embedded data, many of which were posted by lawyers who ostensibly should have been aware of embedded data.

These facts suggest that lawyers are not aware of metadata; whether their failure is due to lack of reasonable care is not yet clearly settled. The only authority on this point rejected imputing lawyers with knowledge of embedded data. Obviously, as awareness of embedded data spreads, it will become more difficult for lawyers to contend that transmitting embedded data did not violate the duty of care. As a result, at some point—perhaps soon—lawyers will not be able to avoid negligence claims by pleading ignorance of the risks that this information creates. However, until that time, whether a lawyer “should have known” will remain a fact-intensive issue, turning on the nature of the practice, the type of representation, and the importance of the information at issue.

The problem, of course, is that a lawyer does not want to be the “test case” which announces that this time has come. Where a lawyer knows or should know of the presence of embedded confidential information, the lawyer must take steps to avoid its disclosure. The next section addresses how to avoid intentionally sending embedded confidential information.

1. How to Remove or Avoid Creating Embedded Data

There are several ways to address inadvertent transmissions of embedded data. This section surveys technical and other means to eliminate or at least reduce the likelihood of an inadvertent transmission occurring.

54. See also Hoenig, supra note 10, at 51 (“Many, if not most, lawyers are unaware that documents prepared with word processing software often contain information invisible to the normal document reader, particularly if the document is read only from a paper printout.”).
55. See Krause, supra note 6, at 27 (describing example containing track changes and comments in Word document).
56. As noted below, this lack of certainty about whether lawyers know or should be deemed to know about embedded data complicates the question of whether lawyers who receive files with their opponents’ embedded confidential information have an obligation to destroy the file, or avoid reading it. See infra notes 71-98 and accompanying text.
57. N.Y. St. Bar Ass’n Comm. on Prof’l Ethics Op. No. 782 (Dec. 8, 2004). See Zall, supra note 17, at 56 (reasoning that attorneys must “exercise reasonable care by familiarizing themselves with the attendant risks associated with metadata and taking affirmative steps to eliminate the risks.”).
58. Some say that day came nearly two years ago. Vincent Polley, chair of the ABA’s Cyberspace Law Committee, has been quoted as saying that lawyers can no longer “plead ignorance when it comes to this stuff anymore.” Krause, supra note 6, at 27.
59. See Walker, supra note 9, at 331 (“When a lawyer transmits a document knowing that its metadata reflects client confidences … and that the non-lawyer recipient is able to reveal the hidden text, and does not take protective measures to strip the document of metadata, the lawyer’s transmission … may constitute a knowing disclosure of client confidences ….”).
60. See generally Levitt & Rosch, supra note 9, at 40 (describing various means to remove metadata, including some of those discussed here); Storm Evans, How to Commit Malpractice With a Computer, 29 L. PRAC. MGMT. 56, 56 (2003) (“If you must e-mail or otherwise deliver a Word document, consider using macros or a utility program to strip away the metadata”).
a. Avoid Creating Embedded Data

One way to avoid disclosure of embedded confidential information is to not create it in the first place. Microsoft has in recent years created updates that allow users to avoid creating embedded data. While this is obviously a sure fix, it also means that lawyers cannot take advantage of the power that functionalities such as “Track Changes” bring to the program. A lawyer could not, for example, exchange revisions of a document with her client using “Track Changes” and “Comments” to render the revision process more efficient and certain.

Nonetheless, if there is no embedded data, it cannot be transmitted. Thus, creating documents with “Fast Saves” off, “Versions” disabled, and without any data in the “Properties” file meets this goal. Similarly, PowerPoint can be configured to remove personal data from the “Properties” file. Finally, in WordPerfect, one can ensure that “Multiple Undoes” is turned off and set the program so that the properties are deleted from the document.

b. Removing Embedded Data

Because embedded data can contain confidential client information, lawyers who transmit files should consider removing it. There are various steps that can reduce, or eliminate, metadata. Because reasonable care is necessary, the nature of the communication will indicate what steps are required for particular communications or practices.

Saving a document into .pdf format reduces the amount of metadata but does not eliminate it entirely. For many purposes, simply saving a document into .pdf format may suffice. However, documents in .pdf format can-
not be easily modified, which may reduce the efficiency and functionality of
document exchanges.

Each of the programs has add-ons and other utilities to remove meta-
data. As you can see, they require several steps per document, and pur-

---

67. There are different approaches for different programs. Here are some basics:

**Microsoft Office XP**


You can also show and remove hidden text:

1. On the Tools menu, click Options, and then click the View tab.
2. Click to select the Hidden text check box, and then click OK.
3. On the Edit menu, click Replace.
4. Click More to expand the dialog box.
5. Click anywhere in the box next to Find what.
6. Click the Format button, and then click Font.
7. Click to select the Hidden check box, and then click OK.
8. Click Replace All.


Once you are finished removing hidden text, you can hide hidden text:

1. On the Tools menu, click Options, and then click the View tab
2. Click to clear the Hidden text check box, and then click OK.

*Id.* (Instructions on how to manually remove your user name, personal summary information, comments, headers and footers, revision marks, hyperlinks, styles, old file versions, links from field codes, template names and locations, routing slip information, VB code names and references, network and hard disk information, and document variable information may also be found at this site).

**PowerPoint 2003**

1. On the File menu, click Save As.
2. In the Save As dialog box, click Tools, and then click Security Options.
3. On the Security tab, click to select the Remove personal information from file properties on save check box, and then click OK.


**WordPerfect 12**

To find and remove all hidden text

1. Click View ▶ Reveal Codes.
2. Click Edit ▶ Find and Replace.
3. In the Find and Replace dialog box, click Match ▶ Codes.
4. In the Codes dialog box, choose Hidden On from the Find codes list.
5. Click Insert & Close.
6. In the Find and Replace dialog box, choose Nothing from the Replace with list box.
7. Click Replace All.
8. Click Close.


To accept or remove document revision annotations

1. Click File ▶ Open.
2. Locate the file that has been reviewed, and click Open.
   The Review Document dialog box will open.
portedly not all embedded data is necessarily scrubbed from the document by taking all of these steps. As a result, reliance on commercial software to do the job may be required under some circumstances, especially where the information is particularly valuable or sensitive.

c. Agreement with Counsel

A final, less technical manner of avoiding the problems associated with embedded data is to have an agreement in place with opposing counsel that any transmission of embedded data is not intentional and will require the opposing party to return files containing embedded data. Obviously, this

3. Click Author.
4. On the Document Review toolbar, click one of the following buttons:
   • [symbol omitted] Inserts the currently selected annotation into the text of the document
   • [symbol omitted] Inserts all annotations into the document text
   • [symbol omitted] Deletes the currently selected annotation
   • [symbol omitted] Deletes all annotations from the document text
5. Click Close.
Id. at 7.
To disable the Undo/Redo history
1. Click Edit ➤ Undo/Redo History.
2. Click Options.
3. Disable the Save Undo/Redo items with document check box.
4. Click OK.
5. Click Close.
Id. at 9.
To remove summary information from an older document or template
1. Click File ➤ Open.
2. Choose the file you want to open, and click Open.
3. Click File ➤ Properties.
4. Click the Summary tab.
5. Delete any information that should not be distributed with the document ...
6. Click OK.
7. Click File ➤ Save.
Id. at 10-11. There are also instructions on how to remove comments, styles, names and initials, hyperlinks, header and footer information, linked objects and instructions on publishing the document as a .pdf. Id. at 3.
68. Id. at 4.
69. There are a number of commercial “metadata scrubber” programs available: see Hoenig, supra note 10, at 51 (explaining that a Google search of “clean metadata from word documents” garnered 18,000 hits); Levitt & Rosch, supra note 9, at 41 (discussing various programs). The programs below relate to Microsoft products. I was unable to find removal tools for WordPerfect. I have never used any of these but list them for your convenience.
   iSpecLegSecureBarMetadata.asp
   iScrub, at http://www.esqinc.com/?p=products&id=2
70. See generally Thomas E. Spahn, Litigation Ethics in the Modern Age, 33 BRIEF 12, 16-17 (Winter 2004) (suggesting such agreements in order to address the risks of inadvertent transmission of
turns on the trust of counsel, and where the mere viewing of the information "lets the cat out of the bag," such agreements may not suffice. Either ensuring that embedded data is not created or that it is stripped out before a file is sent will, in most circumstances, be the only effective way to address the problems of embedded data.

d. Using Paper

Based upon experience and discussion with others, there is not one sure-fire way to remove all embedded data all of the time. Transmitting paper, not electrons, may be the only certain way to avoid unknowingly transmitting embedded confidential information. Obviously, though, that defeats the functionalities of software and denies lawyers the convenience of the Internet.

B. The Obligations of Lawyers Who Receive Inadvertently Transmitted Information from Opposing Parties

The foregoing shows that it is unclear whether lawyers who transmit embedded data do so "intentionally," or in violation of the duty of confidentiality. Further, some embedded data may constitute privileged or confidential information.\(^7\) It is therefore possible that a lawyer can receive embedded data from opposing counsel that is privileged or confidential and be unable to tell whether it occurred intentionally (which seems doubtful) or inadvertently (which is more likely). In that case, it will be unclear whether the transmitting lawyer sent the embedded data as the result of failing to scrub the data, inadvertently using the scrubber, inadvertently allowing the data to be created in the first place, or ignoring the existence of embedded data. What must the recipient do?

1. The General Duties of Lawyers Who Receive Misdirected Privileged or Confidential Information.

There is an entire body of law directed to the question of the duties of a lawyer who receives a communication by mistake. In some jurisdictions, the lawyer is free to use the materials, even if they contain privileged or confidential information, while in other jurisdictions 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 next.\(^7\)

It is important to note that an ethical responsibility arises when a lawyer receives information that he should know was not intended for him: "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." 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." Significantly, at least under Model Rule 4.4(b), the duty is not limited to documents which contain privileged or confidential information, but instead applies whenever a lawyer receives a document that he should know was sent inadvertently, regardless of the content. Nothing in Model Rule 4.4(b) limits its application to documents that contain privileged or confidential information. Thus, in jurisdictions in which Model Rule 4.4(b) is adopted, a lawyer who receives "a document" inadvertently must notify the sender. Whether intentional receipt of a document that inadvertently contains embedded data implicates this rule is discussed below.

Other authorities take a narrower, or at least different, approach to this issue than Model Rule 4.4(b). Ethics opinions in other jurisdictions impose duties upon lawyers who receive inadvertently transmitted documents from another lawyer, but often only if the document contains "privileged" or "confidential" information. These bar opinions are largely imprecise, based on indeterminate rules (whether, for example, the lawyer "should know" the information was sent inadvertently), not uniform among jurisdictions, and not in effect in every state. In these jurisdictions, a lawyer who receives a document containing embedded data has a duty to notify the party who transmitted the document only if the transmission is "inadvertent" and embedded data is "privileged" or "confidential."

73. MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2004).
74. MODEL RULES OF PROF'L CONDUCT R. 4.4(b) cmt. 2 (2004).
75. In this regard, the rule is broader than some ethics authorities, which impose an obligation to take action only if the information is confidential or privileged. See, e.g., Ethics Op. 2003-04, supra note 72 (concluding that when a lawyer receives misdirected documents containing "confidences" or "secrets," certain obligations arise). Thus, in jurisdictions which impose a duty only when certain types of information are disclosed, a threshold issue of whether the embedded data reflects privileged or confidential information arises. In the abstract, metadata is not likely to reflect privileged information, but comments and track changes likely do. Whether a particular document's embedded data is "privileged" or "confidential" obviously turns on the specific facts.
76. See MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2004).
77. Id.
79. Ethics Op. 2003-04, supra note 72 (concluding that a lawyer who receives misdirected documents must, if they contain "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 (holding that lawyers should assist in preserving confidences of sender of inadvertently privileged documents); ABA Ethics Op. 92-368, supra note 1 (holding that recipient of misdirected communication should advise sender of the mistake and abide by its instructions).
Thus, under either approach, the threshold question is whether the intentional transmission of a document that inadvertently contains embedded data is “inadvertent for purpose of these rules.” Under Model Rule 4.4(b), that alone is sufficient to trigger the notification obligation.81 Thus, the next section addresses what inadvertence means in the context of embedded data.

2. Is Transmission of Embedded Data Inadvertent?

It is important to be clear about what was done inadvertently and what was done intentionally. The assumption is that the lawyer who created the file intended to send it to the lawyer who received the file but unintentionally included embedded data. Can this be characterized as “inadvertent” transmission when it is clear the lawyer intended to transmit the file?

The authorities generally recognize two forms of inadvertent transmission. One occurs when a lawyer inadvertently includes as a recipient an unintended person,82 such as by sending a fax intended for a client to opposing counsel.83 Lawyers must take reasonable precautions to prevent inadvertent transmission of confidential information to third parties, and especially, opposing counsel.84 The harm, of course, is that inadvertent disclosure of privileged information can waive the privilege – or if not, it can let the cat out of the bag.85

Another form of transmission occurs when a person who lacks authority to do so intentionally transmits privileged information to an opposing party.86 This has happened frequently when disgruntled employees mail opposing counsel privileged or work product documents.87 It is more appropriately labeled unauthorized transmission, rather than unintentional transmission, since certainly the disgruntled employee intended to send the information, but was not authorized to do so.

82. The ABA mentioned inadvertent transmission of e-mail when analyzing waiver of privilege over a misdirected fax: “the availability of xerography and proliferation of facsimile machines and electronic mail make it technologically more likely that 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.” ABA Formal Op. 92-368, supra note 1 and accompanying text. Accord Fla. St. Bar Ass’n Comm. on Prof’l Ethics Op. 93-3 (Feb. 1, 1994) (“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.”).
83. ABA Formal Op. 92-368, supra note 1; accord Fla. Ethics Op. 93-3, supra note 82 (“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”).
84. Model Rules of Prof’l Conduct R. 1.6 cmt. 17 (2004) (“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.”).
86. See, e.g., In re Shell Oil Refinery, 144 F.R.D. 73 (E.D. La. 1992) (current employee of a party provided an adverse party with confidential documents belonging to his employer).
87. See, e.g., id.
Although embedded data could be transmitted without authority, it is more likely to fall under the first type of inadvertent transmission. The analogy between transmission of embedded data and inadvertent transmission in the "real world" is fairly obvious: a lawyer intentionally sends a proposed contract to opposing counsel, but inadvertently includes a mark-up of the contract with handwritten comments received from the client. No one would contend that by intentionally transmitting the proposed contract, the lawyer intentionally transmitted the client's mark-up. The lawyer intended the transmission, but he did not intend to transmit the mark-up.

The distinction, of course, is that the embedded data is not a separate file, but is "in" the intentionally sent file. That is too fine a point, and conflates intentionally transmitting a "file" with intentionally transmitting the information the file contains. The transmission of embedded data should be found to be inadvertent.

As a consequence, in states that follow Model Rule 4.4(b), a lawyer who receives a file with embedded data is in a position where receipt alone triggers the rule. As a result, she cannot examine the data, and should notify the sender of its receipt. 88

The only bar association to have addressed this issue agreed with this conclusion. 89 The New York State Bar Association reasoned that, although the transmitting lawyer intended to transmit the file, "absent an explicit direction to the contrary counsel plainly does not intend the lawyer to receive the 'hidden' material or information." 90 It then characterized the transmission as inadvertent, and the review as deliberate, in order to conclude that a lawyer cannot review embedded information; "it 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." 91 As a result, "attorneys who receive electronic documents from the opposing side and take affirmative steps of . . . mining the document for confidential metadata . . . run a substantial risk of" violating the ethics rules or becoming "the target of disqualification motions." 92

Some lawyers who disagree with this conclusion apparently assume that the transmission was intentional, and thus not inadvertent. "The first thing [lawyers] often do when they get documents from the opposition is to look for metadata to see who last drafted it or look for embedded versions of earlier drafts." 93 To support this view, many contend that the transmission

88. *See supra* notes 72-81 and accompanying text.
90. *id.*
91. *id.*
92. Zall, *supra* note 17, at 57-58. The party who sent the document could move to disqualify the lawyer in connection with the matter or substantially related matters, for example. *See* MODEL RULES OF PROF'L CONDUCT R. 1.9 (2004).
93. Krause, *supra* note 66, at 31 (quoting Vincent Polley, Chair of the ABA's Cyberspace Law Committee) (bracketed material in original).
of embedded data is itself an intentional act, since "every one knows" embedded data exists.\textsuperscript{94}

The problem is that whether the transmitting lawyer knew the information exists is irrelevant; instead, the question is whether the recipient should know that the transmission was inadvertent: "The issue thus becomes whether the Inquirer knows, reasonably believes or should know that the disclosure was inadvertent. If the disclosure was not inadvertent then the Rule [4.4(b)] does not apply."\textsuperscript{95} Therefore, in jurisdictions which follow Model Rule 4.4(b), the fact that embedded data was inadvertently transmitted is, by itself, sufficient to trigger the obligations.

Under Model Rule 4.4(b), receipt of embedded data alone triggers the rule and is not limited to inadvertent receipt of documents with privileged or confidential information. Even in those states that limit the ethical obligations to the inadvertent receipt of communications that contain confidential or privileged information, some embedded data will likely be confidential or privileged. For example, every lawyer knows that the opposing side's client's comments on a proposed contract are information that should be kept confidential.\textsuperscript{96} A lawyer, therefore, who knows that viewing the "tracked changes" in a document will reveal confidential information of the opposing party does not mean that the recipient can view that information. Indeed, it means the opposite:

In this regard, information that is clearly identified as confidential in nature or appears on its face to be subject to the attorney-client privilege under circumstances that make it clear it was not intended for the receiving lawyer, should not be examined. The receiving lawyer should immediately notify the sending lawyer and abide by his instructions with respect to inadvertently disclosed privileged material.\textsuperscript{97}

A lawyer who deliberately takes steps to view embedded data is engaging in a deliberate review of information that she ostensibly knows should have been removed, and which she knows is confidential, at a minimum. Further, the transmitting lawyer may not—and indeed, apparently did not—know of the existence of embedded data, or it would have been removed.\textsuperscript{98}

\textsuperscript{94} Some say that day has already come. For example, Vincent Polley, chair of the ABA's Cyberlaw Committee has been quoted as saying that lawyers can no longer "plead ignorance when it comes to this stuff any more." Krause, supra note 6, at 27. See Levitt & Rosch, supra note 9, at 41 (explaining that if the New York opinion were written "today, it may not be as forgiving of a lawyer who fails to remove metadata before sending electronic documents to the opposition").


\textsuperscript{96} Hoenig, supra note 10, at 51 ("When drafting transactional documents, it is obviously undesirable to let the other side see what text was added or deleted...or what changes were being considered for addition or deletion to the last draft of a document sent to the other side that were not included. Disclosing such information to the other side can help it in its negotiation strategy").


\textsuperscript{98} See supra notes 82 to 98 and accompanying text.
Therefore, a lawyer should not view embedded data in jurisdictions where any review of inadvertently transmitted documents is unethical or in jurisdictions that prohibit review of privileged or confidential information of the opposing party.

IV. AN IMPORTANT CONCLUSION

The conclusion that receipt of embedded data triggers ethical obligations in states that follow Rule 4.4(b), and that it triggers obligations in states that adopt the narrower approach to the problem when it contains privileged or confidential information, does not end the inquiry. The lawyer who receives the information can—and, perhaps must if the facts warrant—contend that the inadvertent transmission of the embedded data constituted a waiver of the protections. There is nothing incompatible notifying the sender of receipt of a misdirected communication as required, and yet contending that privilege was waived due to that fact. Indeed, in order to satisfy both the ethical duties imposed in many jurisdictions and the duty of zealous representation of the recipient’s client, the lawyer may need to avoid use of the document and request guidance from a court, if possible.

To return to our Macrosoft example, the lawyer who received the file with the embedded data may, depending on the jurisdiction’s approach to the question of inadvertent receipt of documents, have an obligation to notify Macrosoft’s lawyers of the transmission and, in some states, to follow their instructions on how to proceed. Nonetheless, the lawyer may be free to argue that privilege has been waived, and to litigate the issue.

Finally, a rather Kafka-esque point needs to be noted. Some lawyers, aware of embedded data, are planting false embedded data in order to mislead opposing counsel or to test whether opposing counsel is viewing this material inappropriately. By planting false embedded data, these lawyers may be able to turn improper use of embedded data against those who do not follow their own ethical responsibilities.

Perhaps Macrosoft’s lawyers had the last laugh. Or, perhaps they have themselves compounded the matter by making false statements to the opposing counsel.

99. See, e.g., Sampson Fire Sales, Inc., 201 F.R.D. at 360. (analyzing whether reasonable steps were taken to prevent inadvertent faxing of privileged letter to opposing counsel).
100. See Krause, supra note 6, at 27.