

MCLE ON THE WEB

(\$20 PER CREDIT HOUR)

TEST # 55

1 HOUR CREDIT

LEGAL ETHICS

To earn one hour of MCLE credit in the special category of Legal Ethics, read the substantive material, then download the test, answer the questions and follow the directions to submit for credit.

Metadata: To Scrub Or Not To Scrub *Steer clear of hidden dangers with good information management policies and the requisite software*

By **ROBERT D. BROWNSTONE**

© 2008. All rights reserved.

The Titanic was sunk not by what was visible above the waterline, but by what lurked beneath the surface. In the stormy seas of electronic-information-era lawyering, what you see when looking at an electronic document is just the tip of the iceberg and metadata is the unseen danger looming below.

Metadata means “data about data” or “information about information.” Both the legal and Information-Technology (IT) worlds now generally define metadata as “information describing the history, tracking or management of an electronic document.”

In recent years, metadata has started to become as familiar to lawyers and judges as it had been to technologists. Indeed, metadata can implicate legal, procedural, technological and ethical obligations. Yet the tech-savvy lawyer can readily learn how to steer clear of the jagged edges that might sink a case or a client relationship.

The three principal metadata categories are: *file system*; *e-mail*; and *document (a/k/a embedded data)*.

FILE SYSTEM metadata tracks when an electronic file was created or last modified and by whom, the folder location in which it is — or has been — stored and perhaps also when the file was last opened and/or printed.

- Various file system metadata “fields” can be readily viewed in Microsoft Office (MS Office) programs such as Word, Excel and PowerPoint by selecting Properties from the File drop-down menu.
- All file types, not just word-processing, spreadsheets and presentations, maintain some file system metadata fields.

- Of particular concern to every lawyer is the potential for inadvertently divulging another client's name. Even if a confidential name or word or phrase is no longer reflected in the "Name" of the file, it can still linger in the "Title" field.

E-MAIL metadata is a sub-category of file-system metadata.

- Some of the many specialized e-mail metadata fields are the omnipresent To, From, Date/Time Sent, Subject and Cc. Those fields are readily apparent to sender and recipient upon opening an e-mail — and often even before it (by eyeballing one's Inbox or Sent Items).
- Other, less transparent e-mail file system metadata can provide additional insight, including the sender's domain, the route a message has traveled and where delays may have occurred between sending and receipt.
- Basic e-mail metadata can be viewed by, for example, opening a Microsoft message and then selecting Options from the View drop-down menu.
- More detailed e-mail metadata often is not viewable in the application used to create the e-mail. Yet, depending on which of the many e-mail systems is being used, various tools — including some at the e-mail database/server level — can be used to view and manipulate this less accessible metadata.

DOCUMENT (IMBEDDED/ EMBEDDED) metadata consists of prior content of an electronic file.

- Examples are: inserted comments, text in trailers and text in small and/or white font.
- This category is the scariest in that, often, the disseminator has no idea that the embedded content was ever, let alone still is, in the file. The reason: The problematic prior content may not be visible when the creator or last reviser/"reviewer" opened, or last edited, the document.
- Once revealed, embedded data can yield major surprises. In each of Word and Excel, one to three clicks can reveal reviewer name(s), the sequence in which changes were made and, at times, the actual contents of those changes.
- In MS Word, some of the ominous scenarios include:
 1. copying and pasting a portion (just some of the cells) of an Excel file yet inadvertently embedding the entire Excel spreadsheet; and
 2. mishandling Tracked Changes.

File system and document metadata are found in many file types, including those in the MS Office family. Even when the context is neither electronic discovery nor even litigation, lawyers should be cognizant of metadata's daily reach. The frequent re-use of prior electronic work-product places all attorneys in the midst of the estimated 90 percent of computer users whose first drafting step is "File . . . Save as" or right-click-copy on a file icon followed immediately by right-click-paste. See Shankland, Stephen, *Hidden text shows SCO prepped lawsuit against BofA*, c/net (Mar, 18, 2004) <http://news.com.com/2102-7344_35170073.html?tag=st.util.print>.

A confounding problem for lawyers and non-lawyers often derives from the misuse of Word's Track Changes feature. Businessman Derrick Max, reacting to Democrats' outrage when his e-mailed Congressional testimony revealed input from the Republican Social Security Administration, vented that, "The real scandal here is that after 15 years of using Microsoft Word, I don't know how to turn off 'track changes.'" Zeller, Tom, Jr., *Beware Your Trail of Digital Fingerprints*, N.Y. Times (Nov. 7, 2005) <http://www.nytimes.com/2005/10/11/07/business/7link.html?pagewanted=print>

There are many other highly publicized examples of embarrassing disclosures. The ranks of those bitten by the cobra of embedded data include the United Nations, the British Prime Minister's Office, the Democratic National Committee, the California Attorney General's office and the Motion Picture Association of America. For details, see Shankland, *supra*; Zeller, *supra*; Gene Koprowski, *Networking: Not-so-secret documents*, UPI (Feb. 6, 2006) <<http://www.physorg.com/news10567.html>>; Brian Bergstein, *Cos., gov't seek to keep lid on metadata*, AP (Feb. 3, 2006) <[http:// Bergstein-AP-2-3-06.notlong.com](http://Bergstein-AP-2-3-06.notlong.com)>.

At least some of those gaffes seem to have resulted from Tracked Changes. How? The creator or modifier of a Word document can err by merely un-highlighting the tracked changes, perhaps by choosing "Final" from the "Display for Review" menu on the "Reviewing" toolbar. Then, any recipient of the file can simply use the same toolbar to re-highlight the changes. The best practice consists of affirmatively accepting and/or rejecting all the tracked changes and then cleaning ("scrubbing") the metadata (*see below*).

There are at least three ways to dig for embedded data (a/k/a metadata "mining"). Low-tech manipulation includes the use of basic drop-down menus in Word, Excel, PowerPoint and Adobe Acrobat. Higher-tech manipulation includes clicking on the "analyze" command in any of the readily available, inexpensive metadata cleaning software. Expert manipulation goes even farther by running eDiscovery software on a batch of files to extract metadata and then search it.

In all areas of law practice, sea-mines are present, whether a given document was drafted by one side or both sides. Any lawyer e-mailing an attachment to opposing counsel, an expert or a client may be breaching confidentiality. Why one's own client? Because Client A likely has no business knowing anything about Client B, even the fact that you are representing Client B. Along those lines, a recent California ethics opinion addressed

the return of electronic documents comprising a client-matter file upon the end of a representation. State Bar of Calif. Standing Comm. on Prof'l Resp. and Conduct (COPRAC), Formal Op. No. 2007-174 (Aug. 14, 2007) <<http://www.calbar.ca.gov/calbar/pdfs/ethics/2007-174.pdf>>. That opinion mentioned a duty to strip metadata reflecting confidential information as to other clients. See generally Brownstone, Robert and Grunfeld, Gideon, *Saying Goodbye Just Got More Expensive Redaction Reaction; Do's and Don'ts*, 29 *The Bottom Line*, No. 2 (Feb. 2008).

Not all metadata contains harmful or privileged information. Yet, when metadata does, inadvertent disclosure can: waive attorney-client privilege and/or work-product; generally jeopardize a client; and hurt the attorney-client relationship. Nationwide, judicial decisions and ethics opinions as to metadata have been evolving scattershot.

As to a recipient's ethical duty, there is a stark split:

■ *View # 1 – Metadata Mining is Forbidden as it may Invade the Sender's Client's Confidences*

SUMMARY: Treats confidential information in metadata like other types of “inadvertently” disclosed information by deeming it unethical to examine (“mine”) a file's metadata without consent of the sending attorney.

ADHERENTS: The Alabama, District of Columbia and Florida bars and the New York State Bar Association (NYSBA).

■ *View # 2 – If the Sender Didn't Scrub Metadata, Fughetabout It!*

SUMMARY: Allows an attorney to ethically view metadata in a file received from opposing counsel. If the sender had wanted to preclude the recipient from mining the metadata, he/she should have used reasonable care by employing scrubbing software.

ADHERENTS: The American Bar Association and the Maryland and New York City bar associations.

As to a sender's ethical duties, however, there is unanimity. All of the above bars' and bar associations' ethics opinions agree that the sender has a “duty . . . to use reasonable care when transmitting documents by e-mail to prevent the disclosure of metadata containing client confidences or secrets.” N.Y.S.B.A. Op. 782, Comm. on Prof'l Ethics (Dec. 8, 2004) <<http://NYSBAOp782.notlong.com>>.

As to the overall issue of inadvertent disclosure — whether or not involving metadata — there is much less consistency as to the recipient's obligations. Some states employ a tortured parsing of who knew what someone else intended — and when. Others naively presume that a remedy can be satisfactory though it is impossible to erase already-read information from a recipient's memory. According to a 2006 survey:

- nineteen U.S. jurisdictions follow the ABA view that the recipient's only duty is to notify the sender;
- eight believe the recipient must immediately stop reading upon realizing a document contains ostensibly privileged information, notify the sender of the error and follow the sender's instructions;
- eight others take other, varying approaches; and
- the final 16 have been silent.

Only three California decisions have squarely addressed inadvertently disclosed privileged material. Two months ago, in the context of hardcopy lawyer notes, our state's highest court held that "an attorney . . . may not read a document any more closely than is necessary to ascertain that it is privileged. Once it becomes apparent that the content is privileged, counsel must immediately notify opposing counsel and try to resolve the situation." *RICO v. Mitsubishi Motors Corp.*, (2007) 42 Cal. 4th 807 <<http://www.courtinfo.ca.gov/opinions/documents/S123808.PDF>>.

Given the Pandora's Box that opens when one has to litigate an inadvertent disclosure dispute, it is best to mitigate the risks in advance. Neither MS Office's menu options nor its free "Remove Hidden Data" (RHD) tool (now called Document Inspector) remove all risky metadata. Thus, the soundest approach is to use metadata-cleaning software to scrub any e-mail attachment before it is sent out into the world from your law firm or legal department. Payne Consulting Group's (PCG's) Metadata Assistant is a basic metadata analysis/removal application that is effective, as is the more powerful Workshare Professional or Workshare Protect. Both PCG and Workshare can be configured to prompt a user each time he/she clicks to send an e-mail outside of your firm or department.

Some rely on tall tales to rationalize foregoing metadata-scrubbing software. For example, many a lawyer thinks he/she (and therefore the client) is wholly protected by an automated conversion of an MS Office file to .pdf format. Yet, even there, at least some file system metadata migrates to the new file. A recipient of a file converted without prior metadata scrubbing can simply input "Ctrl+D." Then, he/she can poke around in the .pdf's properties to identify the Title and Author borne by the file when in its original format.

To avoid that migration scenario, scrub the original file before or during its conversion to .pdf. And maybe after as well. Adobe Acrobat 8.0's "Examine Document" feature removes metadata.

Similarly, conversion to .pdf does not magically fix — but, rather, perpetuates — an improperly handled electronic redaction. Given that a federal eFiling exposes a .pdf to anyone in the world with a PACER number, the stakes are even higher. Electronic

redaction — even more significant in light of brand new Fed. R. Civ. P. 5.2 — is beyond our scope. For a detailed exploration, see Brownstone, Robert, Gregorian, Todd and Sands, Michael, *Secrets Easily Leaked by Friend or Foe In Publicly Filed .PDF Documents*, 9 No. 10 E-Commerce L. Rep. 7 (West Oct. 2007), available at http://www.fenwick.com/docstore/Publications/IP/IP_bulletins/IP_Bulletin_Fall_2007.pdf

Follow the “Three E’s” — Establish, Educate and Enforce — by: 1. creating overall information management policies; 2. appropriately training employees; and 3. deploying requisite software. For some of the benefits and potential contours of an information regime, see Brownstone and Grunfeld, *supra*.

Now you have the navigational equipment necessary to avoid those hidden dangers. Stay alert at the helm, and avoid metadata mishaps. Bon voyage!

■ *Robert D. Brownstone, the Law & Technology Director at Fenwick & West LLP in Silicon Valley, is a member of four state bars, the Information Systems Auditing and Control Association (ISACA) and the executive committee of the State Bar’s Law Practice Management and Technology (LPMT) Section. Fenwick & West paralegal Robert Winant assisted in the preparation of this article.*

Test — Legal Ethics
1 Hour MCLE Credit

This test will earn one hour of MCLE credit in Legal Ethics.

1. “Metadata mining” is the act of intentionally seeking and viewing metadata in an electronic document received from opposing counsel.
2. The majority of states are silent regarding a recipient’s ethical obligations after receiving inadvertently disclosed, apparently privileged information from opposing counsel.
3. It is generally considered to be the sending attorney’s ethical duty to use reasonable care when e-mailing an attachment containing metadata.
4. The California State Bar has opined that an attorney is ethically obligated to take reasonable steps to strip metadata from electronic items being forwarded to one client when that metadata reflects confidential information belonging to any other client.
5. Embedded metadata is always revealed upon opening a document.
6. Microsoft’s Document Inspector is the best tool for removing metadata.
7. Only Microsoft Office files contain metadata fields.
8. Problems with metadata only arise when sending electronic files to adversarial parties.
9. Most e-mail metadata is usually contained within the visible header fields, such as To, From, etc.
10. California courts have issued numerous decisions regarding inadvertently disclosed privileged material.
11. The best way to avoid inadvertent disclosures of metadata is to use an appropriate scrubbing/cleaning program on electronic files.
12. The Supreme Court of California recently decided that, upon sensing that a document received from opposing counsel contains privileged information, an attorney’s first response must be to zealously represent his/her client by reading the rest of the document.
13. The best way to strip metadata from a word-processing, spreadsheet or presentation file is to convert it into a PDF file.
14. Methods exist to view special e-mail metadata, including the sender's domain, the route a message has traveled over the Internet, and where delays may have occurred between sending and receipt.

- 15.** Only electronic forensic experts have the tools to review embedded/document metadata.
- 16.** The two types of metadata are Email and File System.
- 17.** When you use the Display for Review toolbar to un-highlight tracked changes in a Microsoft Word document and then e-mail that document to another user, the recipient is not able to view the Tracked Changes without special forensic tools.
- 18.** By inputting Ctrl-D while in a .PDF file whose metadata was not scrubbed when it was a word-processing file, a user can view the Title and Author of the original file just prior to its conversion.
- 19.** When using a prior document as a drafting starting point, using the File. . . Save As command protects the user from any accidental exposure of prior content of the original file.
- 20.** Conversion to .pdf format alleviates any errors in electronic redaction when the file was in word-processing format, such that the .pdf version is safe for eFiling with a court.

Certification

- This self-study activity has been approved for Minimum Continuing Legal Education credit by the State Bar of California in the amount of one hour of legal ethics.
- The State Bar of California certifies that this activity conforms to the standards for approved education activities prescribed by the rules and regulations of the State Bar of California governing minimum continuing legal education.

MCLE ON THE WEB

TEST # 55 — Metadata: To Scrub Or Not To Scrub

1 HOUR CREDIT
LEGAL ETHICS

- Print the answer form only and answer the test questions.
- Mail only form and check for \$20 to:

MCLE ON THE WEB — CBJ
The State Bar of California
180 Howard Street
San Francisco, CA 94105

- Make checks payable to State Bar of California.
- A CLE certificate will be mailed to you within eight weeks.

Name

Law Firm/Organization

Address

State/Zip

State Bar Number (required)

1. True___ False___
2. True___ False___
3. True___ False___
4. True___ False___
5. True___ False___
6. True___ False___
7. True___ False___
8. True___ False___
9. True___ False___
10. True___ False___

11. True___ False___
12. True___ False___
13. True___ False___
14. True___ False___
15. True___ False___
16. True___ False___
17. True___ False___
18. True___ False___
19. True___ False___
20. True___ False___