

METADATA: TECHNOLOGY CREATES NEW THREAT TO CLIENT CONFIDENTIALITY

JANUARY 12, 2006

Rule 1.6 of the *New Hampshire Rules of Professional Conduct* provides in part that “a lawyer shall not reveal information relating to representation of a client unless the client consents after consultation ...” The proliferation of technology in the practice of law has created the potential for violations of this rule, and injury to the interests of clients, that may not be readily apparent to the average practitioner. One such risk arises through the electronic sharing of word processing, spreadsheet and other document files that contain embedded information known as “metadata.” Metadata is the data “behind” the document, which is not readily viewable by the reader.

The Nature of “Metadata”

Most commonly-used word processing and spreadsheet programs, as well as other application programs that allow editing and annotation, embed hidden information in each saved document file. As lawyers, we review metadata on a regular basis during the editing of electronic documents. Depending on the particular software application that was used, this metadata can include such things as:

- Date on which the document was first created
- Computer name of the device on which the document was created
- Original source of the document
- Location of the document
- Author of the document
- Company and department with whom the author is employed
- Version /revision numbers

Attorney Conduct & Liability Practice Group

Peter Beeson, Chair
603.695.8517
pbeeson@devinemillimet.com

Mitch Simon, Of Counsel
603.228.1541
msimon@devinemillimet.com

Andy Dunn
603.695.8503
adunn@devinemillimet.com

Bob Dewhirst
603.695.8646
rdewhirst@devinemillimet.com

Betsy Baker
603.695.8699
bbaker@devinemillimet.com

DEVINEMILLIMET.COM

- Name and location of template files used to create the document
- Names of users on document routing slips
- Dates on which the document was accessed
- Dates on which the document was edited or modified
- Dates on which the document was printed
- Printer name and path for the device on which the document was printed
- Names of the users who accessed, edited, and saved the document
- Total document editing time
- Tracked changes in the document, including additions and deletions of content
- User comments and notations added during the editing process
- Category, keywords and descriptive comments used to profile the document
- Embedded objects, such as pictures and spreadsheets
- Hidden spreadsheet text, worksheets, data columns and data rows
- Speaker notes

As can be seen from reviewing this list, there is a wealth of unseen (but by no means undiscoverable) data that can potentially attach to a document when transmitted to a third party. Whenever a user shares a copy of such a document with opposing counsel, a client or another party outside the firm, (whether by means of electronic mail transmission or via some magnetic storage medium, such as a floppy disk), that rich hidden data set is passed to the recipient along with the document.

If the information remained hidden, it would not present a potential ethical problem for attorneys. However, this metadata can be easily recovered (or “mined”) from a document using third-party software that is readily available - - in some cases at no cost. Anyone using this software can, with a minimal amount of technical expertise, recover metadata that would not otherwise be available to someone reviewing the document. The recovery of this data by persons for whom it was not intended, could potentially result in the disclosure of attorney/client privileged information, sensitive work product, or other confidential information.

Office Locations:

111 Amherst Street
Manchester, NH 03101
T 603.669.1000
F 603.669.8547

300 Brickstone Square
Andover, MA 01810
T 978.475.9100
F 978.470.0618

49 North Main Street
Concord, NH 03301
T 603.226.1000
F 603.226.1001

216 Lafayette Road
Suite 103
No. Hampton, NH 03862
T 603.964.4990
F 603.964.4997

The Risks Posed by Unauthorized Access to Metadata are Real

The unintended release of metadata is not a speculative problem, as the following real life incidents show.

“British” Dossier is Really American: One very real and highly-publicized incident involving metadata occurred in February of 2003, when the British government published a dossier on Iraq’s security and intelligence organizations. When the dossier, which was made available in Microsoft Word format on a British government web site, was examined by a lecturer at Cambridge University, the source and editing history revealed that much of the document had been copied directly from materials prepared by a U.S. researcher. (It has been reported that the British government no longer publishes its documents publicly in word processing format.)

Florida Bar Condemns Metadata Mining: Only last month, the Florida Bar Association Board of Governors had occasion to condemn the practice of mining for metadata. Their action followed a report from the president-elect of the Bar that an appellate brief provided in electronic format by his firm to another lawyer had been mined by the recipient - disclosing privileged work product and client communications. The Board voted unanimously to approve a motion presented by the Board Review Committee on Professional Ethics clearly expressing that attorneys should not engage in the practice of metadata mining. In addition to condemning the practice of metadata mining, the Board voted to refer to the Ethics Committee two questions for their formal consideration: whether it is unethical for a lawyer to mine metadata from an electronic document received from another party; and whether an attorney has an affirmative duty to take reasonable precautions to remove sensitive metadata from an electronic document prior to transmitting it to third-parties.

Metadata Results in Disciplinary Referral: A final, recent metadata incident receiving attention on a few of the legal profession Internet list servers involves a professional conduct complaint made by a client against his/her own attorney. Allegedly, after receiving a copy of a word processing file, the client reviewed the editing information contained in the document’s metadata, and concluded that billing for the work on the document has been improper. A professional conduct complaint followed.

* * *

These actual reported incidents are, almost certainly, only the tip of the iceberg. It is not difficult to envision other scenarios in which significant harm to the client could result from the transmission of metadata to opposing counsel (or to third parties):

- An attorney collaborates with a client on the preparation of a complex contract. As the document evolves, it shuttles electronically between attorney and client. At each stop, additions and deletions are redlined and editing comments made. When the document has been completed, the display of the redlining and comments is disabled, and it is transmitted electronically to opposing counsel for review. Upon receipt, opposing counsel or his/her client can mine the metadata contained in the document - - gaining an enormous negotiation advantage through access to the thought process contained in the editing history of the document and the comments made by the drafting parties.
- An attorney copies an estate plan that was originally prepared for one client, and uses it to prepare a similar document for a second client. The first client's information is deleted and replaced with the new client's data during the editing process. Upon completion, the new document is sent electronically to the second client for review. The client can, if so inclined, mine the metadata in the document, revealing the first client's confidential testamentary plan.
- Several attorneys representing a single party collaborate on the preparation of a document production response. As the response is prepared, the attorneys exchange comments regarding the advisability and obligation of producing (or withholding) certain documents. Some of the comments reflect a difference of opinion within the producing counsel's firm as to which documents should be produced. When finalized, the document is transmitted to opposing counsel with the comments disabled. Opposing counsel mines the metadata and gains access to the producing counsel's comments. A motion to compel (seeking sanctions) follows.

As can be seen from the foregoing hypothetical scenarios and actual incidents, the risk of disclosing confidential information is real. The dissemination of electronic documents (whether to opposing counsel, clients, or third parties) carries with it the potential for inadvertent disclosure of confidential client information,

as well as the thought processes and mental impressions of counsel. Such a disclosure would, at a minimum, be professionally embarrassing to an attorney. Under some circumstances, it could cause significant harm to the interests of clients.

Recent Ethics Opinions on the Metadata Issue

As of the date of this Advisory, there are no published New Hampshire cases or ethics opinions that address the issues raised by the inadvertent disclosure of privileged material contained in metadata. However, the New York Bar Association Committee on Ethics has issued two opinions that are directly on point. (Links to these opinions and other resources can be found below.)

In Opinion 749, the Committee opined that a lawyer may not ethically utilize technology to trace e-mail messages, or to discover other electronic information hidden in e-mailed documents sent by opposing counsel. In reaching this conclusion, the Committee reasoned that discovery of data that was never intended to be disclosed by the sender constituted an impermissible invasion of the attorney-client privilege. The Committee also stated that the exploitation of an unauthorized communication of confidential information would constitute conduct involving “dishonesty, fraud, deceit or misrepresentation,” and “prejudicial to the administration of justice,” in violation of New York’s ethics rules.

In Opinion 782, the same Committee was asked to consider whether an attorney “knowingly” reveals the confidences or secrets of a client by e-mailing documents that contain metadata reflecting privileged client information. In its opinion, the Committee observed that an attorney who uses technology to communicate with his or her clients must assess the risks attendant to the use of that technology, and determine if the mode of transmission is appropriate under the circumstances. The Committee opined that the sending attorney has a duty to exercise reasonable care with respect to such transmission, noting that “reasonable care may, in some circumstances, call for the lawyer to stay abreast of technological advances and the potential risks in transmission in order to make an appropriate decision with respect to the mode of transmission.”

Although the New Hampshire Bar Association Ethics Committee has not yet issued an opinion addressing the risks of

metadata, the positions taken in the two New York ethics opinions, and by the Florida Board of Governors, are not surprising, and should cause any New Hampshire attorney who communicates electronically with clients and/or opposing counsel to assess carefully the risk of an inadvertent disclosure of privileged information via the metadata contained within those communications.

Is There a Solution?

Fortunately, the threat posed by metadata can be easily minimized. Inexpensive software is available which will quickly and completely remove all sensitive metadata from word processing and other data processing documents. Attorneys who share electronic documents with parties outside their offices should install one of the available metadata scrubbing utilities, and adopt the firm-wide practice of purging outgoing documents of their metadata, where warranted, prior to the dissemination of those files outside of the firm. By implementing such a policy, and by becoming sensitive to the types of privileged information that may be hidden within word processing, spreadsheet and other data files, attorneys will reduce significantly the possibility of unintended disclosure of confidential client matters.

Links to Resources:

1. [New Hampshire Rules of Professional Conduct, Rule 1.6](#)
2. [New York State Bar Association, Committee on Professional Ethics, Opinion 782, December 8, 2004](#)
3. [New York State Bar Association, Committee on Professional Ethics, Opinion 749](#)
4. [Production, Preservation, and Disclosure of Metadata, by James Brian Beckham, John Marshall School of Law, Ohio University, June 2005](#)
5. [*Beware Your Trail of Digital Fingerprints*, The New York Times, Tom Zeller, Jr., NYTimes.com, November 7, 2005](#)

6. *Microsoft Word Bytes Tony Blair In The Butt*, Richard M. Smith, June 30, 2003
7. *Control Metadata In Your Legal Documents*, Microsoft Office Online
8. *Tech Toolbox Survey*, Massachusetts Bar Association, October 2003

The Advisories on the Law of Lawyering in New Hampshire issued by the Attorney Conduct & Liability Practice Group are intended to provide general overviews of professional responsibility law in a variety of areas encountered by lawyers. Because the law in this field is constantly changing, and because the Advisories are generic, they should not be relied upon as guidance or advice on how to handle specific situations. If you have any questions about this e-mail, or if you know of anyone else who may be interested in receiving these alerts, please send us an e-mail at AC&LPG@devinemillimet.com.