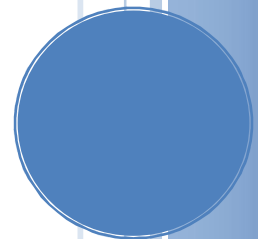


California Law Firms and Metadata Policies

As more states sound off on metadata and an attorney's responsibility, California firms with practices in multiple states should also make sure that their policies are acceptable in every jurisdiction in which they practice.

By Randall Farrar
Published in the GLA ALA
Leadership Exchange Aug/Sept 2010

ESQUIRE
INNOVATIONS, INC.



CALIFORNIA LAW FIRMS AND METADATA POLICIES

In states across the U.S., including California, governing bodies have drafted and issued opinions regarding an attorney's professional responsibility regarding metadata. Historically, opinions on whether there is a significant risk with metadata and if so, what must be done to address that risk have varied between attorneys, IT departments, management, bar associations and other governing entities. With increasing opinions specifically addressing an attorney's ethical obligations regarding metadata, law firms must now address their management of metadata and develop specific policies or update existing policies to ensure they are in accordance. As more states sound off on metadata and an attorney's responsibility, California firms with practices in multiple states should also make sure that their policies are acceptable in every jurisdiction in which they practice.

In 2007, the California State Bar Standing Committee on Professional Responsibility and Conduct issued Opinion No. 2007-174, which examines the ethics duties of attorneys regarding metadata.

"An attorney is ethically obligated, upon termination of employment, promptly to release to a client, at the client's request" documents. Further "the attorney is ethically obligated to take reasonable steps to strip from each of these electronic items any metadata reflecting confidential information belonging to any other client."

For the complete opinion, visit

<http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=kiSRjKqnMBg%3D&tabid=838>.

For more information on other states opinions regarding an attorney's professional responsibility regarding metadata, visit

<http://www.abanet.org/tech/ltrc/fyidocs/metadachart.html?ecamp=t-r128>

Given the California Bar's opinion that an attorney has an ethical duty to prevent disclosure of "any metadata reflecting confidential information belonging to any other client," law firms without a metadata policy or with an outdated policy must address the firm's policies to ensure that they are exercising reasonable care when transmitting documents.

There are three key components to developing a metadata policy - Establish, Enforce and Educate. However, before a firm puts pen to paper, it is important that those tasked with writing a policy understand what metadata is and where it is found.

WHAT IS METADATA?

Succinctly defined, metadata is “data about data.”

Microsoft Word, Excel and PowerPoint include automated features to aid in document production and collaboration. These features embed electronic information (metadata) in a file which can reveal the identity of those who edited the document (revision authors); track the time, date, and frequency of edits (track changes and revisions); reveal inserted comments and the document template; and other data employed to control the document’s text and format. It is the commonly held opinion that this information should be removed before a file is shared outside the firm’s electronic walls to avoid violating attorney client privilege, disclosing sensitive information to third parties and so on.

Many people think of tracked changes when they think of metadata. There have been numerous high profile cases where tracked changes inadvertently left in a document have had embarrassing, not to mention legal and ethical consequences. This mistake can be easily made. An attorney switches on the Track Changes function to make edits to a document. After collaborating with his assistant and associates, he is satisfied with the changes. He decides to send it to the client for review by changing the document to “Final” in the “Tracking” section.

The tracked changes disappear from the document. He assumes they are no longer there, clicks on Send via e-mail and sends the document to his client. The client opens the document to see all of the tracked changes displayed. This happened because the attorney did not accept all of the changes in the document; he merely hid them from view. When the client opened the document her “Display for Review” settings were set by default to “Final Showing Markup”, thus revealing all of the changes in the document. If the firm had a metadata policy in place that detailed when documents are “cleaned” before being sent externally, this situation would have been avoided.

The metadata contained in a Word document other than the intended text doesn’t necessarily create risk of adverse disclosure. In fact some document metadata is necessary for formatting or automation macros within a document. Some document metadata, such as tracked changes, may be used to collaborate with co-counsel, but would not want to be shared with adversarial counsel.

To make sure there are no tracked changes in your document, always accept all changes. However, there is also an extra security feature in Word that warns you when you have tracked changes in your document when you print, save or email a document.

To turn Word's Track Changes warning system on, follow these steps:

- On the Office button Select "Word Options."
- In the Word Options dialog box select "Trust Center."
- In the Options dialog box, select "security" from the list on the left hand side, and then click on the "Trust Center Settings" button.
- Under Document Specific Settings- Click the check box "warn before printing, saving or sending a file that contains tracked changes or comments."

(Note: if your firm uses a metadata software this feature should probably be turned off since it may interfere with the software. Check with your vendor first).

For added security, click the check box "Make hidden markup visible when opening or saving." This will ensure that tracked changes are always visible.

Two examples of high profile metadata blunders are the SCO Group's lawsuit against DaimlerChrysler and a United Nations report. In the SCO lawsuit, a Microsoft Word document from SCO's suit against DaimlerChrysler originally identified Bank of America as the defendant instead of the automaker. More info on the blunder can be found by visiting http://news.cnet.com/2100-7344_3-5170073.html.

In a United Nations report tracked changes were discovered in a document that supported the published conclusion that Syria was behind an assassination in Beirut. More info can be found by visiting, http://www.timesonline.co.uk/tol/news/world/middle_east/article581486.ece.

A rule of thumb when understanding metadata is that every time a document is opened, edited and saved metadata is added by the application, the operating system or the user. While track changes may provide an obvious example, there are many other scenarios when metadata can cause problems for a law firm.

For example, an attorney is creating a contract for a new client. The contract requires some standard language. Since she has prepared similar contracts before, the attorney opens a contract created previously for another client in Microsoft Word, when she worked at a different firm. Using "Save As" she saves the document under a new name, makes edits as needed and e-mails it to her client. Upon receipt the client opens the document and, since they have heard about metadata, opens file properties to view any

data. (File properties can be accessed in Office 2007 by clicking on the “Office Button | Prepare | Document Properties | Advanced Properties”). By viewing the “Statistics” tab the client sees a “Created” date of one year before they were a client and a “Modified” date of the date the attorney emailed the document. Even more puzzling in the “Summary” tab they see a different firm listed in the “Company” field. The client now has access to a history that reveals information the attorney should have not revealed. That history will stay with the document until it is “cleaned” using a metadata management tool.

Metadata of this type can be useful when searching for documents created in a specified time frame, or to gain quick access to documents from, for example, My Recent Documents. But a firm may not want to reveal this type of information to a client being billed time for creating the document.

Metadata also exists in Excel files. In Excel, metadata can also be very useful and can include formulas in a spreadsheet (a powerful feature for editing and calculating figures), hidden columns, author names and creation dates of documents. All can reveal information not intended for general distribution. In Excel, formulas can be useful but if spreadsheets are linked to other workbooks, links should be disabled and formulas changed to static numbers before sending out, to prevent revealing information not intended for general distribution.

In PowerPoint, metadata also includes author information and presentation creation dates as well as speaker notes and links to graphs or other statistics from outside documents. Again, information you may not want to share.

ESTABLISHING A METADATA POLICY

- Educate yourself about metadata and review the Bar’s ethics opinion (and other states and entities, as needed) regarding metadata.
- Review firm documents (on internal networks and published on external networks). Is your firm inadvertently sharing confidential informations?
- Involve attorneys and your IT department and established a firm approach based on your findings.
- If necessary, bring in a consultant to advise your firm on a metadata policy.
- Moving forward, review your policy on a routine basis to address any new rulings on metadata.

ENFORCING THE POLICY

Consider purchasing metadata management software. The software you choose should be flexible enough to execute firm policy, automated enough to enforce firm policy and easy enough for users to understand and utilize.

The latest Microsoft Office program includes a metadata tool called “Document Inspector.” Since Microsoft applications add metadata to files, it presents a somewhat contradictory position for Microsoft to provide a tool for removing that metadata. Firms who already practice a metadata policy have found the main weakness with Document Inspector is the lack of automation. The onus is on individual users to “inspect” documents and then decide the metadata to remove, proving to be ineffective in enforcing a metadata policy throughout an organization.

Metadata management software, on the other hand, removes metadata more thoroughly and is designed to help firms automate and therefore, enforce metadata policies. The most popular products available for metadata management can be found by searching for “metadata management software” in Google.

EDUCATING A LAW FIRM

The success of any policy hinges on the execution. A firm’s metadata policy will be more successful if staff can grasp what metadata is, when it can be useful, when it can be harmful and how to manage the metadata in documents. Consider bringing in outside trainers to help educate your firm with hands on training.

About The Author: *Randall Farrar is the president and cofounder of Temecula, CA- based Esquire Innovations, Inc. (www.esqinc.com), a software company that develops Microsoft Office integrated applications for the legal market. Esquire’s products include iScrub 7, a metadata management application for Microsoft Office used by over 450 law firms and corporations; iCreate 7, its popular document production and formatting software; iRedline 7, enhanced Word document comparison; and iDocID, software for adding a document ID to a Word or Excel document. Together, the four products are available as the combined package iOffice 7. He can be reached at Randall.farrar@esqinc.com*