

Vermont Law Firms and Metadata Policies

Across the United States, including Vermont, governing bodies are drafting and issuing 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 an increasing number of 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, Vermont firms with practices in multiple states should also make sure that their policies are acceptable in every jurisdiction in which they practice.

In 2009, the Vermont Bar Association Professional Responsibility Section issued ethics Opinion 2009-1 that states: "... the Vermont Bar Association Professional Responsibility Section finds nothing to compel the conclusion that a lawyer who receives an electronic file from opposing counsel would be ethically prohibited from reviewing that file using any available tools to expose the file's content, including metadata." The Section suggests that such a rule would limit "the ability of a lawyer diligently and thoroughly to analyze material received from opposing counsel." The Section states that, under VRPC Rule 4.4(b), "Vermont lawyers are subject to the obligation to notify opposing counsel if they receive documents that they know or reasonably should know were inadvertently disclosed."¹

According to the opinion, Vermont attorneys have a duty to use reasonable care when transmitting metadata. Citing the "virtually unanimous" view on the topic amongst other bar associations, Vermont

agrees that, based upon the language of the [Vermont Rules of Professional Conduct], a lawyer has a duty to exercise reasonable care to ensure that confidential information protected by the attorney client privilege and the work product document is not disclosed. This duty extends to all forms of information handled by an attorney, including documents transmitted to opposing counsel electronically that may contain metadata embedded in the electronic file.²

The Section does not address whether inadvertent disclosure via metadata constitutes a waiver of a document's privileged status. That is a "question of substantive law" and the Section's research did not reveal "any case law in Vermont addressing the impact of inadvertent disclosure of privileged documents."³

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 given the task of 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.

A rule of thumb for 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 in which metadata can cause a law firm problems. 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 up 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 she has 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 she was a client and a "Modified" date of the date the attorney e-mailed the document. Even more puzzling, in the "Summary" tab she sees 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. Examples include: formulas left in cells; hyperlinks to other workbooks; and hidden rows, columns, or worksheets. All can reveal information not intended for general distribution.

In PowerPoint you may not want to share presentation notes or comments attached to a presentation. You can also embed hyperlinks to graphs or Excel workbooks in a

presentation, which, if left, will link back to the original document. Again, information you may not want to share.

Establishing a Metadata Policy

- Educate yourself about metadata and review the Vermont Bar's ethics opinion (and those from 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 information?
- Involve attorneys and your IT department, and establish 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 that already have 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; this proves 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.

Randall Farrar is the president and co-founder of Esquire Innovations, Inc. (esqinc.com), a software company that develops Microsoft Office integrated applications for the legal market, located in Temecula, CA. He can be reached at randall.farrar@esqinc.com.

¹ VBA Sec. on Prof'l Responsibility, Ethics Opinion 2009-1 (2009), available at <http://69.39.146.6/Upload%20Files/~/WebPages/Attorney%20Resources/aeopinions/Advisory%200Ethics%20Opinions/Electronic%20Documents/09-01.pdf>. 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>

² Ethics Opinion 2009-01, *supra* note 1.

³ *Id.*

