



Metadata – Are you Protected?

By Donna Payne, Payne Consulting Group

Guarding Against Threats

In today's world of legal computing law firms have to constantly protect themselves from any number of security threats. Malicious computer viruses and scripts, hackers and even spyware designed to 'secretly' record your every keystroke and send that information to marketers and other third-party interests are just a few of the daily issues IT administrators face. The threats are as varied and numerous as they are real. Firewalls and other security related software must constantly be updated in order to protect law firm networks from being compromised. As we become increasingly connected through the use of e-mail, handheld devices, instant messaging and other communication driven technology, the issue of security becomes ever more critical.

Do you know what's in your documents?

In most law firms, legal secretaries and attorneys have a general idea of the principal risks and issues associated with network security. IT departments often send out periodic reminders regarding internet and e-mail policies and regularly apply security patches and other updates. Many firms have developed best practices and procedures for computer usage which are posted on the firm intranet or employee handbook and are also covered with newly hired employees. But how many legal users are aware of the dangers posed by sending out documents electronically? Amazingly – fewer than you might think

It has been estimated by several independent sources that more than 90% of all documents are created electronically. Long gone are the days of sending files out in hardcopy and waiting for the client to send back a revised copy via snail mail. Today, documents are created and sent out electronically for review and revision with little thought to what might be in them other than what is visible to the naked eye.

Word Documents and Metadata

Microsoft Word (and Excel and PowerPoint) documents contain 'hidden' information known as metadata. Some types of metadata are benign and useful while other types can provide others who view or work on your documents with information you may not want them to know. Every time you create or edit a Word file, certain types of hidden information are stored with and travel with the document. This can include the list of the last ten authors, the amount of time spent editing the document, changes that have been made to the document as well as the name of the attached template, custom document properties and much more.

It's in WordPerfect and PDF Files Too

Many legal professionals who are knowledgeable regarding the issues and risks associated with metadata in Word files are often surprised to learn that WordPerfect and PDF files also contain

large amounts of hidden information. Rather than purchase and deploy third party metadata removal tools, many law firms simply advise users to publish external documents as PDF files before sending; under the assumption they will be 'metadata free.' Sadly this is not the case. PDF files contain substantial metadata. Sherry Kappel, Vice President of Development at Microsystems explains, "Adobe's integration to Microsoft Office apps provides us *unparalleled* electronic publishing capabilities -- but with those capabilities come heightened responsibilities: are tracked revisions accepted? comments suppressed? document information up to date? redaction techniques electronically savvy? Without checklisting these issues within your document workflow, QC processes and job configuration, a PDF file is as much the "swimsuit competition" as sending the editable .doc file itself. The least revealing 'electronic paper', then, is also the least functional: printing the document to paper, then scan it into PDF."

Table 1.1 reflects a partial list of metadata that can exist in PDF, Word, and WordPerfect files.

(Partial List)

PDF	Word	WordPerfect
• Authors	• Authors	• Authors
• Create Data	• Firm Name	• Firm Name
• Filename	• File Locations	• File Location
• PDF Version	• File Properties	• File Properties (Summary tab)
• Page Count	• Fast Saves	• Undo/Redo History
• Encryption status	• Versions	• Versions
• Permanent ID	• Tracked Changes	• Tracked Changes
• Changing ID	• Comments	• Comments
• Producer	• Hidden Text	• Hidden Text
• Creator	• Embedded Objects	• Non-visible portions of embedded OLE objects
• Custom Fields	• Hyperlinks	• Hyperlinks
• Title	• Styles	• Styles
• Subject	• Headers and Footers	• Headers and Footers
• Keywords	• Linked Objects	• Linked Objects
• Modification Date	• Small Font	• Small Font
• Bookmarks (Total number)	• Matching Font	• Matching Font
• Annotations (total number, type and total type amount)		
• Page One Size		
• Font Name, Type, Embed Status		

Reducing Your Risk of Exposure

Using a third-party tool such as Metadata Assistant that integrates with e-mail and document management software can help to reduce the risk of accidental exposure. Microsoft offers a free but unsupported Remove Hidden Data utility that is available from their web site which can also help to identify potential risks. While third-party add-ins will automate the clean up process, you can also take precautions for minimizing metadata in all applications.

Minimizing WordPerfect Metadata

Corel has published an article about how to minimize metadata in WordPerfect (www.support.corel.com and search “*minimizing WordPerfect metadata*”. The following are just a few steps that you can take to reduce your exposure risks.

- Comments – You can remove a comment by right-clicking on it and clicking Delete, or by viewing reveal codes and dragging the comment code out of the reveal codes window. To prevent comments from containing metadata, from the Tools menu, choose Settings, Environment. Select the General tab and delete the information from the Name and Initials boxes. Unfortunately, the time and date that the comment was made is not removed even when this option is configured.
- Disable Undo/Redo History – The Undo/Redo option in WordPerfect saves and stores historical information about edits made in the document. To disable this feature, from the Edit menu, choose Undo/Redo History. Click Options and disable the Save Undo/Redo Items with Document check box. Click OK, then Close.
- Summary Details – From the File menu, choose Properties and select the Summary tab. Remove the descriptive name, type, creation date, author and other information that you do not want saved with the document.

Minimizing Word Metadata

Word 2002 and 2003 contain security options that are designed to remove some embedded metadata, and show whether track changes or comments exist in a document. To display and configure these options, from the Tools menu, choose Options, and select the Security tab.

- Remove Personal Information From File Properties on Save. When checked, most of the information in the File Properties dialog box is removed, as is the last ten authors and the file path where the document is stored.
- Warn Before Printing, Saving Or Sending A File That Contains Track Changes Or Comments. When checked, this option forces Word display a warning when a document containing tracked changes or comments is being saved, sent, or printed.

- Make Hidden Markup Visible When Opening Or Saving. If a document contains markup and the Reviewing toolbar filter is set to Final, or Original, this security option forces the changes to be visible on Open or Save.

These three settings only remove or identify a small set of the potential metadata in a document. For a more complete solution, you should consider implementing a third-party solution such as Payne's Metadata Assistant.

Minimizing PDF Metadata

There is at least one third-party utility to help eliminate the risk of PDF metadata. Appilgent has a PDF Utilities and Power Tools page with utilities for cleansing metadata from Adobe Acrobat files. www.appligent.com/products/applications/utilities/appligent_utilities.html#apgetmetadata.

Metadata Ethics and Opinions

As metadata and electronic discovery become more prevalent in the courts and in case law, more rules are added to codify the practice of electronic discovery. Currently rules are in place in Texas, New Jersey (Federal District Court), Arkansas, California, Florida, Illinois, Maryland, Wyoming, and in New York (read *Opinion 749 – 12/14/01: Code: DR 1-102(A)(4), DR 1-102(A)(5), DR 4-101, DR 7-102(A)(8), Canon 4, Canon 7, EC 4-1, Lawyers may not ethically use available technology to surreptitiously examine and trace e-mail and other electronic documents.*) More states are researching and implementing new rules on electronic evidence.

Attorneys need to be aware of what rules on electronic discover and what types of information that are sending and receiving. Ross Kodner of MicroLaw has launched a tour railing on the malpractice and ethical risks of metadata. Says Kodner, "the metadata issue is in the public mainstream so lawyers cannot claim "techno.ignorance" of it. Sending metadata-filled documents on behalf of clients would seem to enable both malpractice claims and ethical violations."

Three questions that need to be asked with respect to metadata are:

1. Do lawyers have a duty to warn clients of the metadata risk?
2. Do lawyers have any kind of duty, in "zealously representing the interests of their clients" to look at the metadata in INCOMING documents?
3. If clients are warned, how do lawyers handle the public relations challenge of explaining why it's taken so long to bring this to light?"

Protecting your firm, your clients, and your practice from accidental disclosure is something that everyone needs to be cognizant of. In the case of metadata, the reality is – what you don't see can hurt you.

For more information on Metadata Assistant, e-mail MetadataAssistant@payneconsulting.com or call 206-344-8966.