METADATA: EXPOSED AND EXPUNGED

Colorado Bar Association

January 24, 2017

Charity Anastasio
Director, Law Office Management Assistance
Maryland State Bar Association

Charity Anastasio is the Director of Law Office Management Assistance at the Maryland State Bar Association. She was in private practice for 5 years and at the Washington State Bar Association's Law Office Management Assistance Program for almost 3 years before she joined the MSBA team September 2016. Charity is the Chair of the Local and County Bar Outreach Committee of the ABA Law Practice Division and a regular contributor to the Bar Bulletin of the MSBA. Reach her at canastasio@msba.org or 443-703-3026.

CONTENTS

METADATA: EXPOSED AND EXPUNGED

WHAT IS METADATA?

Metadata is often called the "data behind the data" or "data about data." It is often information about the persons and places that have touched the document, the frequency and different iterations. Not all metadata is harmful and whether it is or not is usually fact specific. But there are some general rules and there are some clear problems with certain types of metadata for the legal profession. It can also be an interesting and helpful tool in a practice that can blow a case wide open, if obtained properly and understood well enough to understand the data available.

Today's CLE will be everything about metadata, but my materials and presentation will focus on the basics. I will discuss what it is, how to find it, how to remove harmful metadata before sharing electronic documents, and why we should care. I will set out some best practices for metadata removal ("scrubbing") with common products used in a law firm, and discuss products that can collect and analyze metadata.

Metadata examples	**Potential exposures**	**Notes**
Author name and other author/collaborator names; contact information	Plagiarism, authorship, collaboration, who is working on case, chain of command, confidences breach.	Last 10 authors automatically saved for 2000 and earlier versions. If converted to later version is removed, and is no longer saved.
Last modified by author; created author	Plagiarism, authorship, collaboration, who is working on case, chain of command, confidences breach.	Accuracy is volatile.
Company name and address; manager's name	Plagiarism, authorship, collaboration, who is working on case, chain of command, confidences breach.	
Creation date; edit dates; last printed date	Billing discrepancies, possible embarrassing information or reuse information.	
Date stamps	When picture or video taken; when a document/item was created.	Virtually all products date stamp creation; versions to varying degrees.
Total drafting time	Billing discrepancies, possible embarrassing information.	
Word count, number of pages	Generally not dangerous	
File size, characteristics	Generally not dangerous	
Tags	Often underutilized function; generally not dangerous unless tags are somehow	

	inappropriate/embarrassing/confidential	
Comments (in document and in properties field)	Strategies, thoughts and opinions, questions, concerns, fact checking, research, etc.	Major source of problems. Easily hidden data
Notes/outline	Strategies, thoughts and opinions, questions, concerns, fact checking, research, etc.	Major source of problems. Easily hidden data.
Redline edits	Strategies, thoughts and opinions, questions, concerns, fact checking, research, etc.	Major source of problems. Easily hidden data
Former versions: Changes made; edits kept, etc.	Strategies, thoughts and opinions, questions, concerns, fact checking, research, etc.	Not automatically saved in newer versions of Microsoft products.
File location	Internal workings, naming conventions	
Embedded information, hyperlinks, formatting, macros, etc.	Strategies, thoughts and opinions, questions, concerns, fact checking, research, etc. Plagiarism, reuse of materials from own or other sources, etc.	
Hidden text, equations, calculations, or cells	Usually Excel issue; could give source data or confidential business information	
Printings: date time, by who	Last printed by which machine, spooling of past printings and by which machine	Stored on printers to varying degree, depending on model, temporary memory capacity, and if powered off or not
Scans: date and time of document name, sometimes the scan	Last scanned by which machine, spooling of past scans and by which machine	Stored on printers to varying degree, depending on model, temporary memory capacity, and if powered off or not
IP/MAC address of devise	Microsoft documents keep record of machine files were accessed and worked on; Geographic location.	Like a social security number for a machine
Browser History/ deleted files/ hidden drafts of documents		Lives on devise unless cleaned out. More of an issue with e-discovery.
Pictures and videos	Camera and what settings shot at, date and time, geographic location depending on devise, size of file	

WHERE TO FIND METADATA?

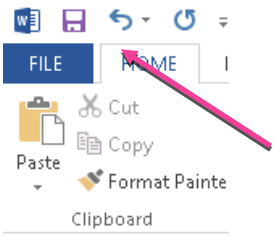
Metadata hides in the background of virtually every electronic format. Here are examples of products that are commonly used in the practice of law that contain potentially harmful metadata. This is not a complete list.

Relevant products	**Devises**
Microsoft Word	Smartphones
Microsoft PowerPoint	Cameras
Microsoft Excel	Laptops
Adobe Acrobat	Desktops
Digital Photographs	Printers
Videos	Scanners
Website pages	Faxes
Email (Microsoft Outlook)	Tablets

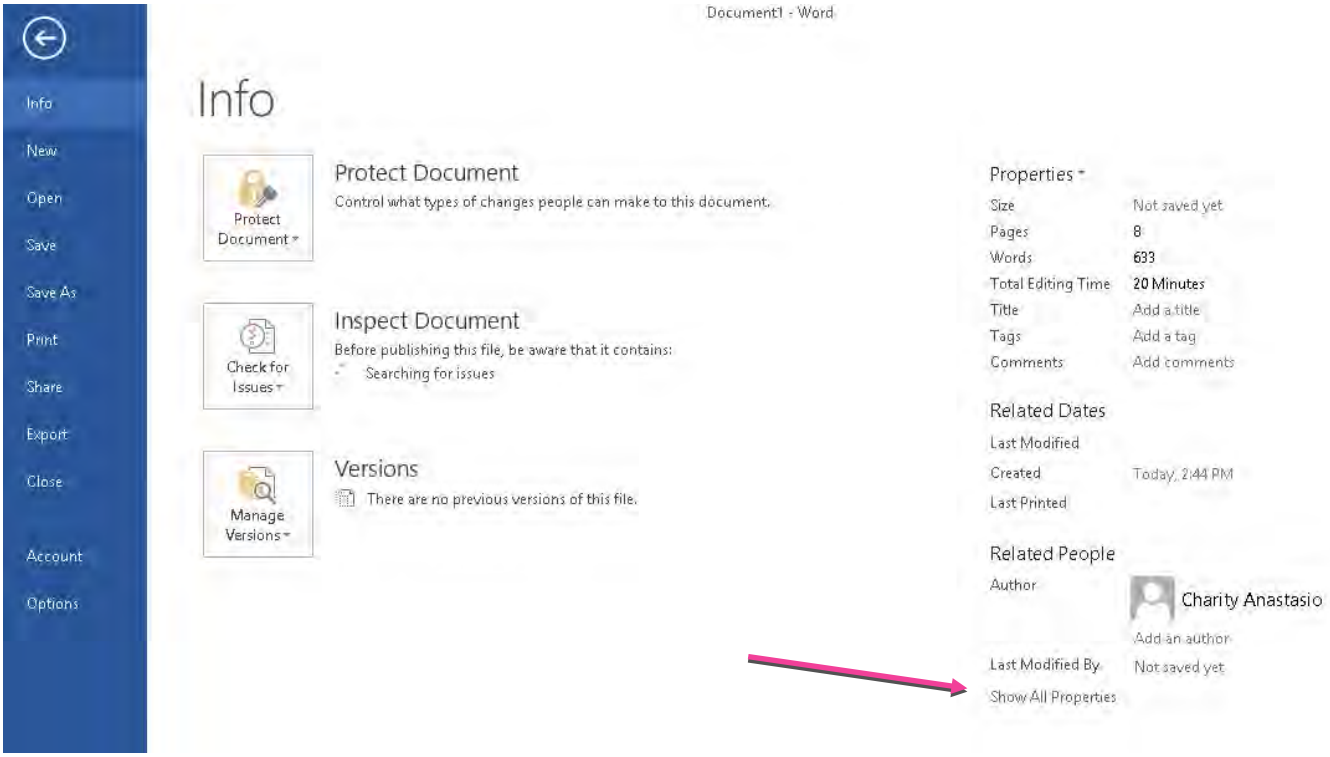
Each product has different ways to locate and remove that metadata. One may find the metadata in the following locations (by product):

MICROSOFT WORD

Microsoft Word location depends on the version being used. In most recent versions the background metadata about the document in can be found by clicking on **FILE** on the top ribbon which brings up the **Info** screen.



From there examine **Properties** and, for the full list, **Show all Properties**.



When one selects **Show All Properties**, it expands to include more information (see below).

The size of the document, how many pages and words it consists of is probably not damaging metadata, and it will stay with the document even after scrubbing.

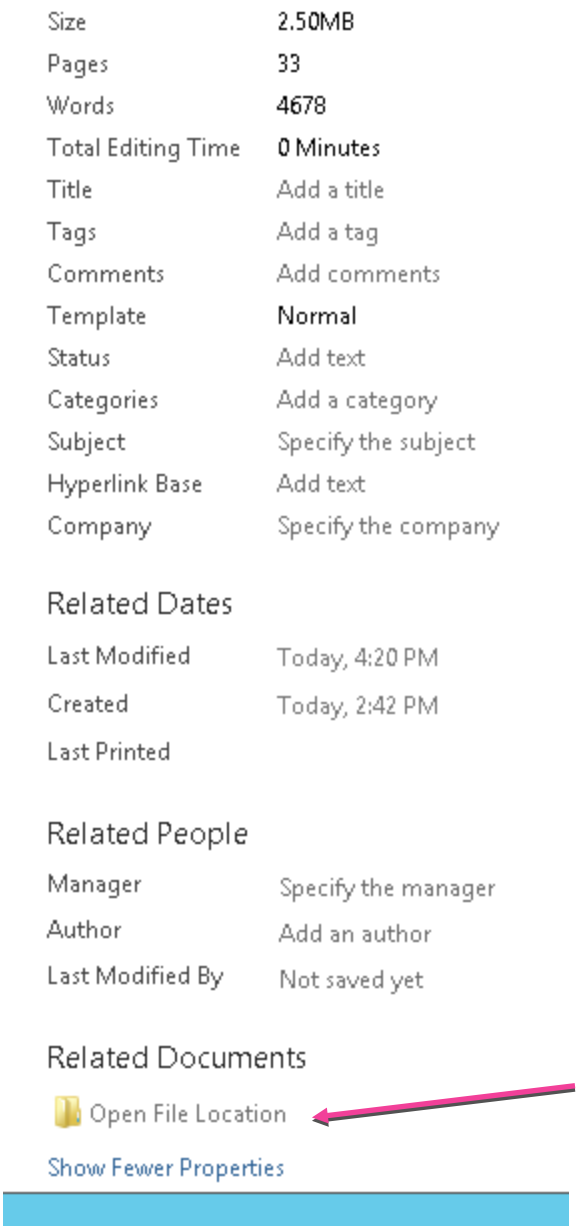
There may be times when the time it took to edit the document is embarrassing or not wanted. This piece of metadata may be inaccurate. It will only be the time that document existed and will not record any time that text was worked on in another document, then copied and pasted into that document.

Usually comments are in the document, but comments and tags may be placed on a Microsoft Word document here as well.

Date stamps include creation date and time, last modified date and time, and last printed time.

A company's name, manager, creator and last editor may show up here. If Wordrake or another add on program is present, this may distort these results.

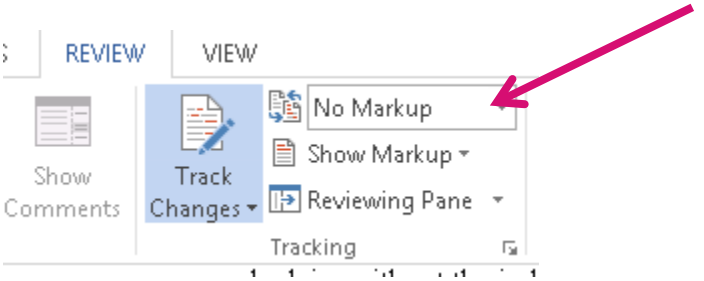
One may open the location of the file from the expanded properties, if one has access and permissions to reach the location.



While most of the properties are probably not dangerous information to disclose, information found in redlining, comments, notes, and previous drafts could be. At best, disclosure is embarrassing and makes folks think the sender is not very tech sophisticated. At worst it could be discloses confidences, strategies, the progression of legal research and argument choice, current or past clients if it is a form that has been used before, or past defendants to a case before they were eliminated (i.e. unethical to committing malpractice).

For the **Comments and Redlined** edits in a document, one need turn on track changes. If these are not removed or "scrubbed" from the document, they can be some of the most damaging forms of metadata in the legal profession to accidentally expose.

In Microsoft Word 2010 there are several options for viewing a document in the Review field of the top ribbon. Here one can add or take off **Show Comments** and **Track Changes,** as well as choose **No Markup**.



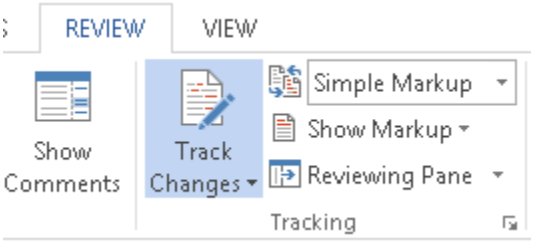
The document will look like this:

12. TERM; TERMINATION

12.1. Term. The "Term" of this Agreement shall commence on the Agreement Date and continue for one (1) year. The term will be renewed automatically unless written notice of termination of the agreement is received within thirty (30) days of termination.

But just because one chose to not see these things does not mean that they are not lurking in the background.

Choose **Track Changes** and **Simple Markup**

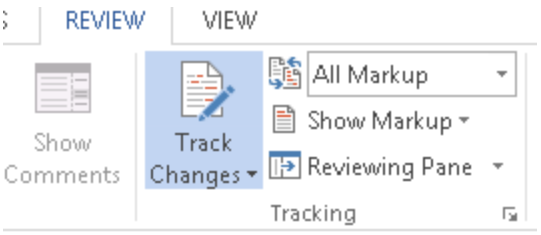


and the document will look like this:

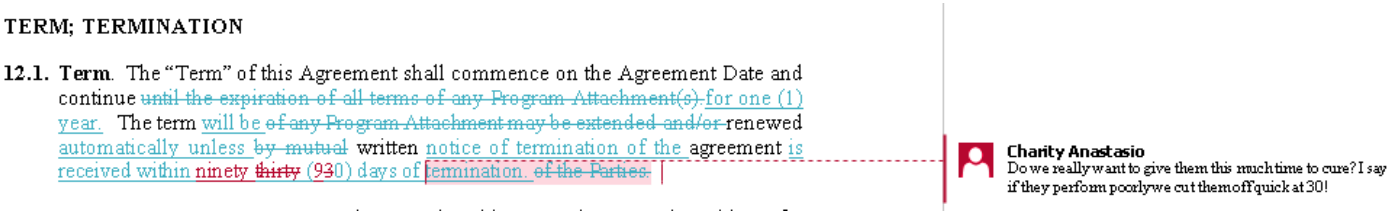
12. TERM; TERMINATION

12.1. Term. The "Term" of this Agreement shall commence on the Agreement Date and continue for one (1) year. The term will be renewed automatically unless written notice of termination of the agreement is received within ninety (90) days of termination.

Choose Show Comments and All Markup

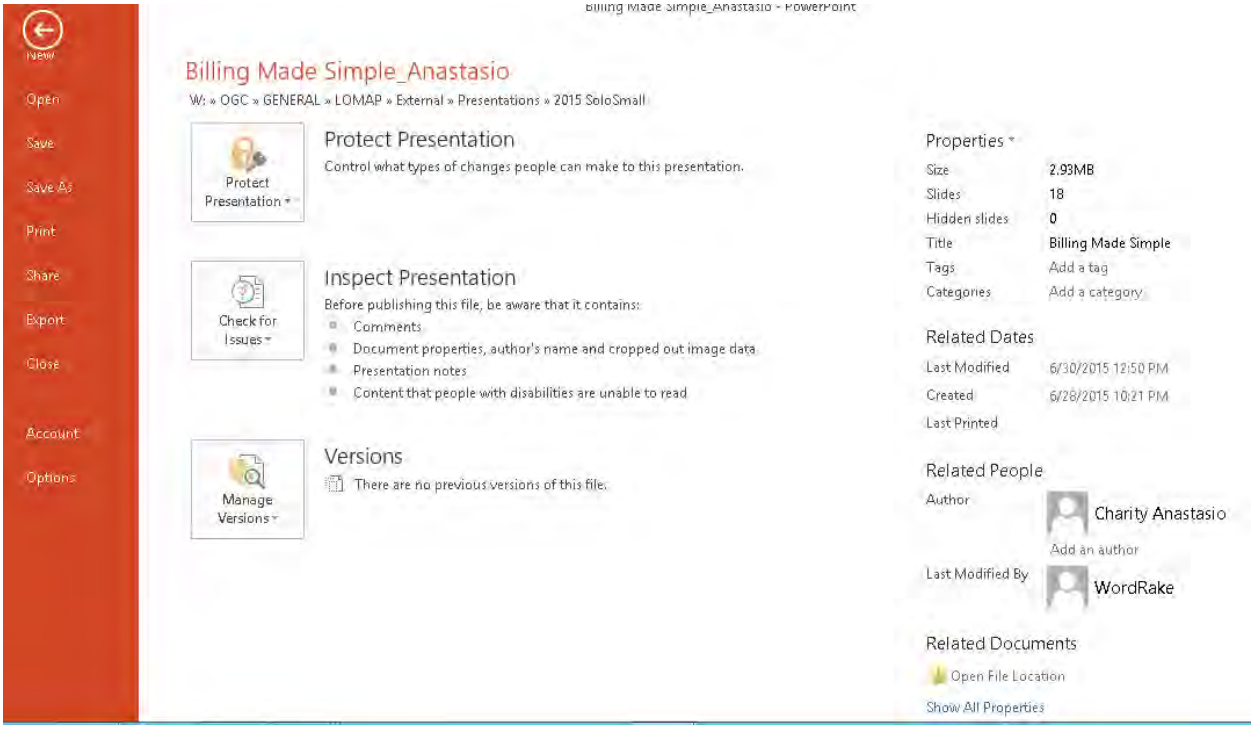


and the same document may look like this:

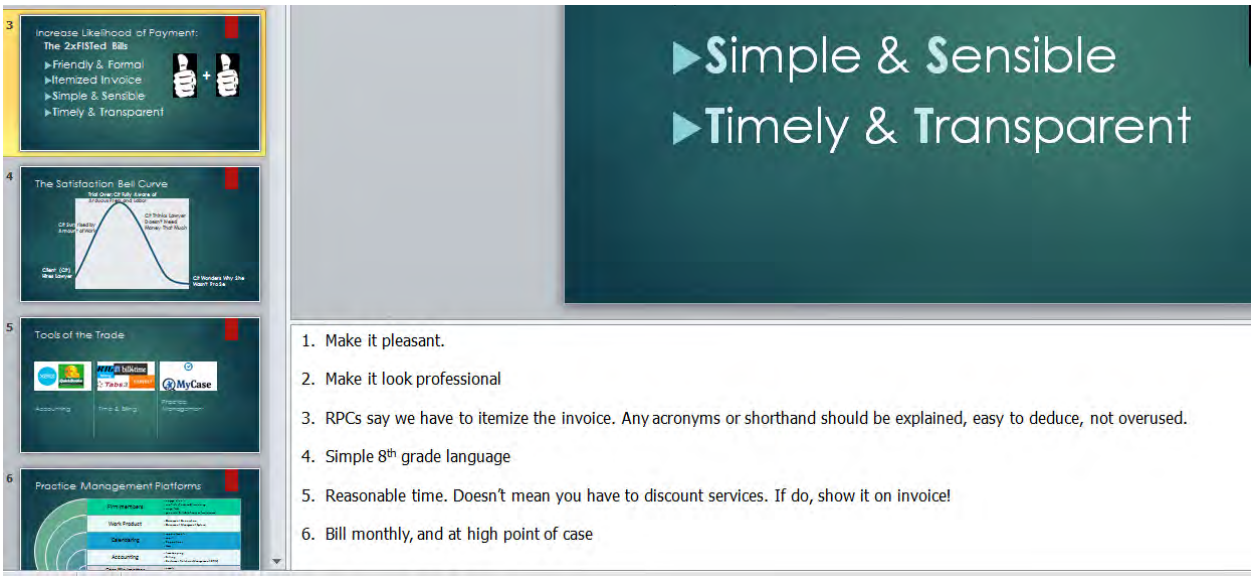


MICROSOFT POWERPOINT

To find the standard metadata is PowerPoint go to **File** and **Properties** (see Word procedure above).

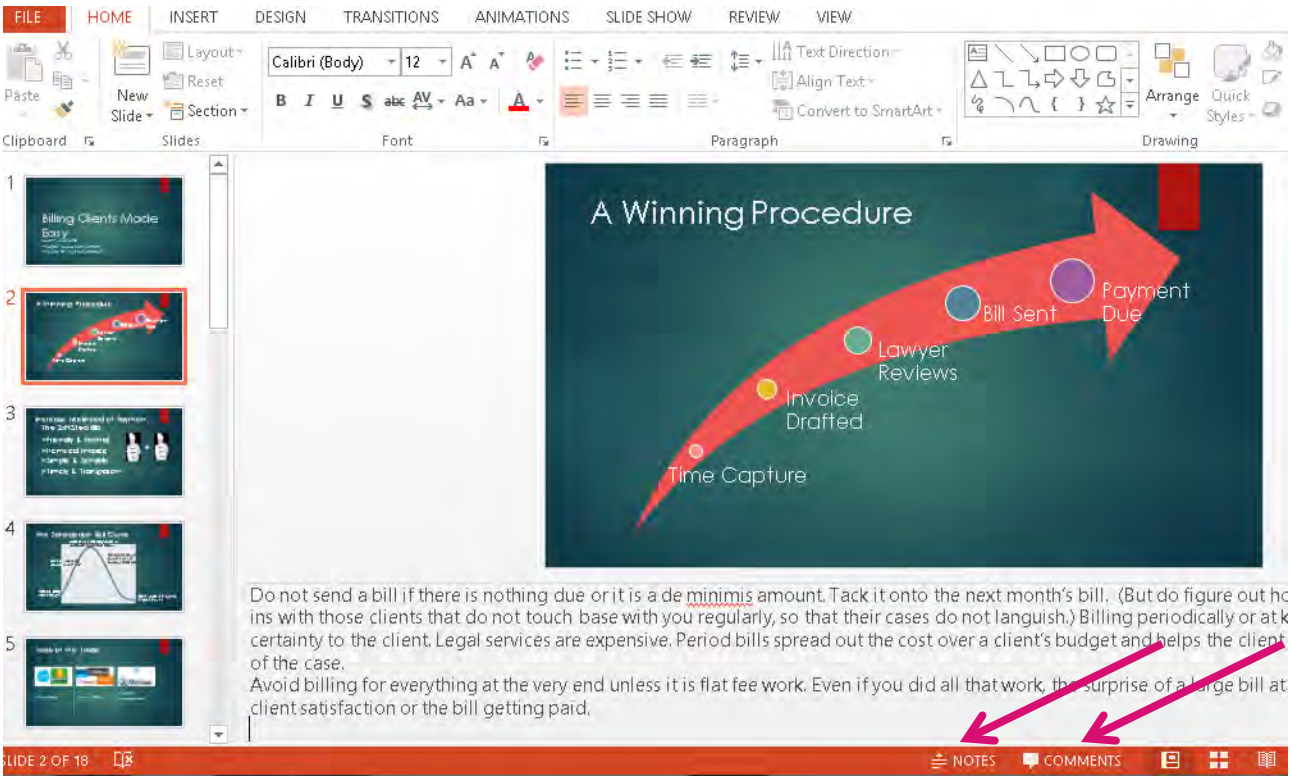


Sometimes authors put **Notes** to follow as they present, or to give background information, like this:

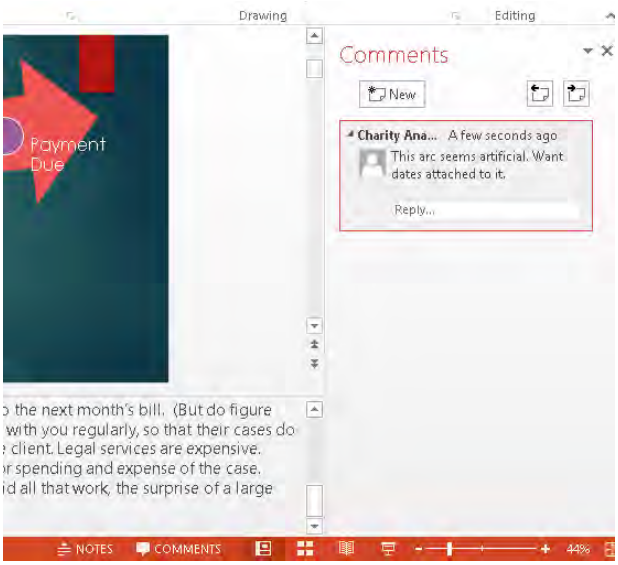


This can backfire if it is confidential or untimely information that is posted publicly or given to the wrong party. This author thinks it is easier to miss comments and notes that are in PowerPoint than it is in Word, maybe because one is dazzled by the pictures and rarely looks at the background information.

The Comments and Notes sections in PowerPoint are easier to find on the online version (Microsoft 365) than on the desktop version, as shown here:



If the notes are not visible click on **Notes** at the bottom of the page.



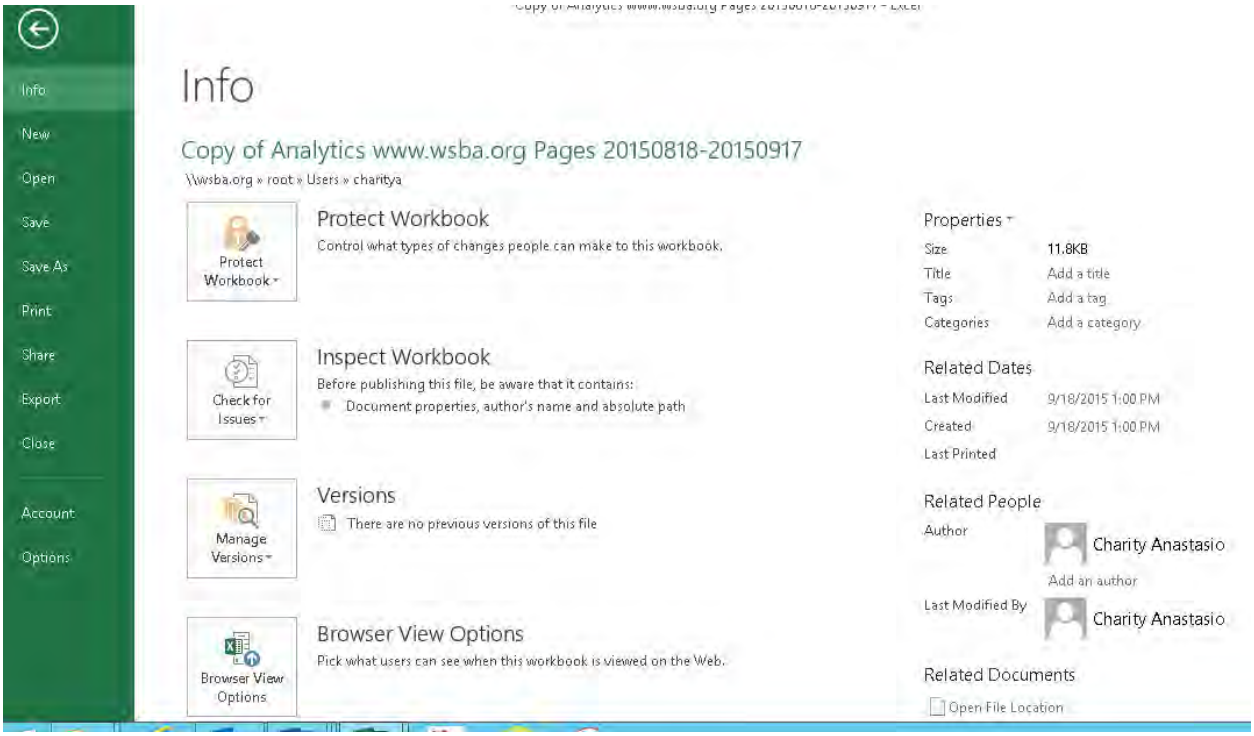
If the comments are not visible, click on comments at the bottom of the page. When there is a comment it will appear on the slide like this:

The online version will also state in red that there is a comment on the slide.

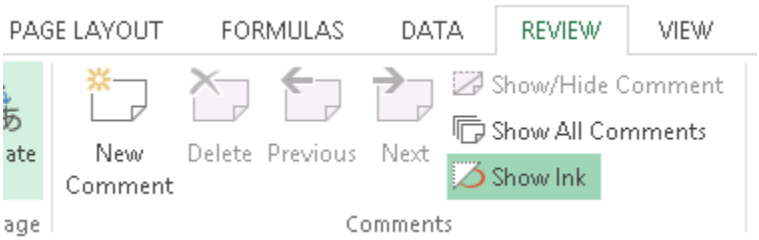
Comments in the desktop 2010 version are more elusive. The comments field at the bottom is only a symbol and the comment is smaller, on the slide. For this reason, it is best to have a scrubbing procedure for every document.

MICROSOFT EXCEL

Excel spreadsheets have wide application and can be linked to different documents, contain telling formulas, and hide comments and notes without much indication that they are there.

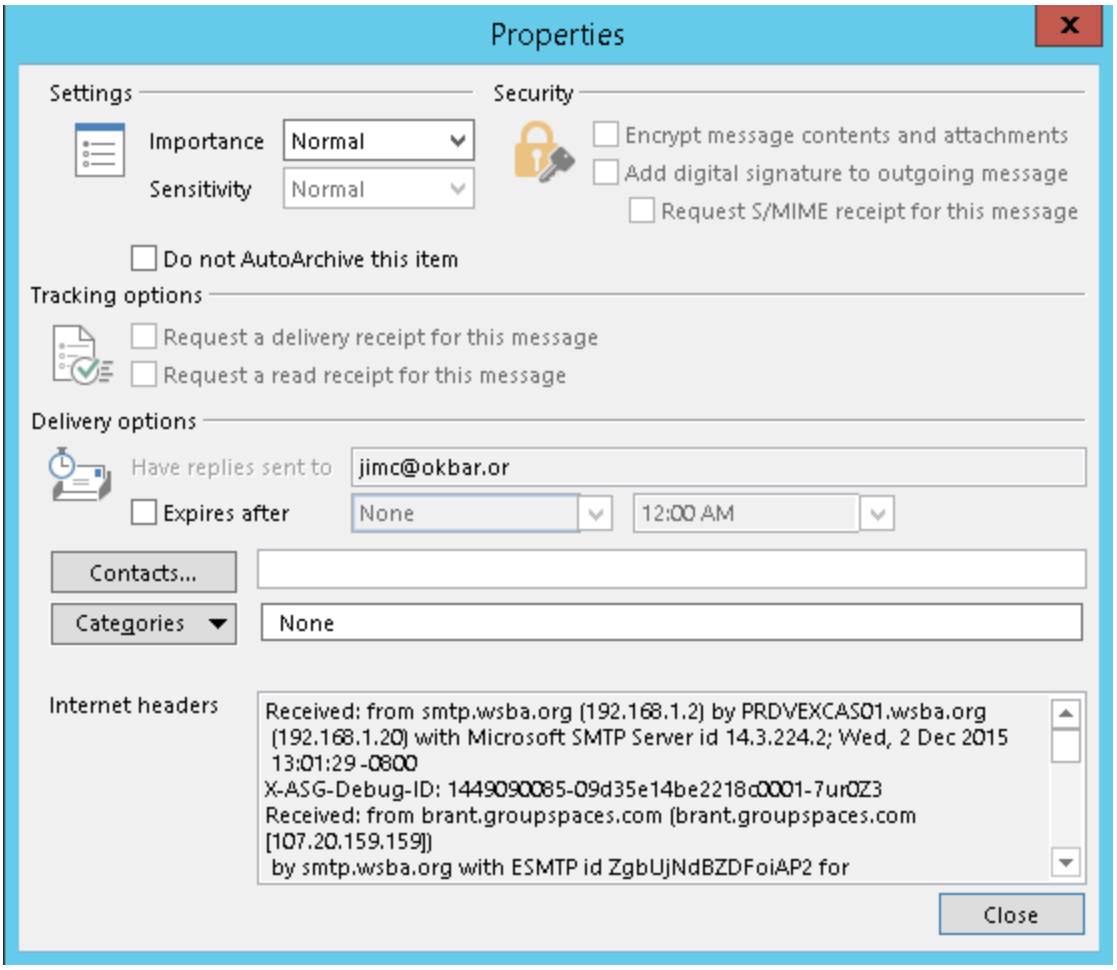


Find linked documents and show comments in the Review panel of the ribbon.



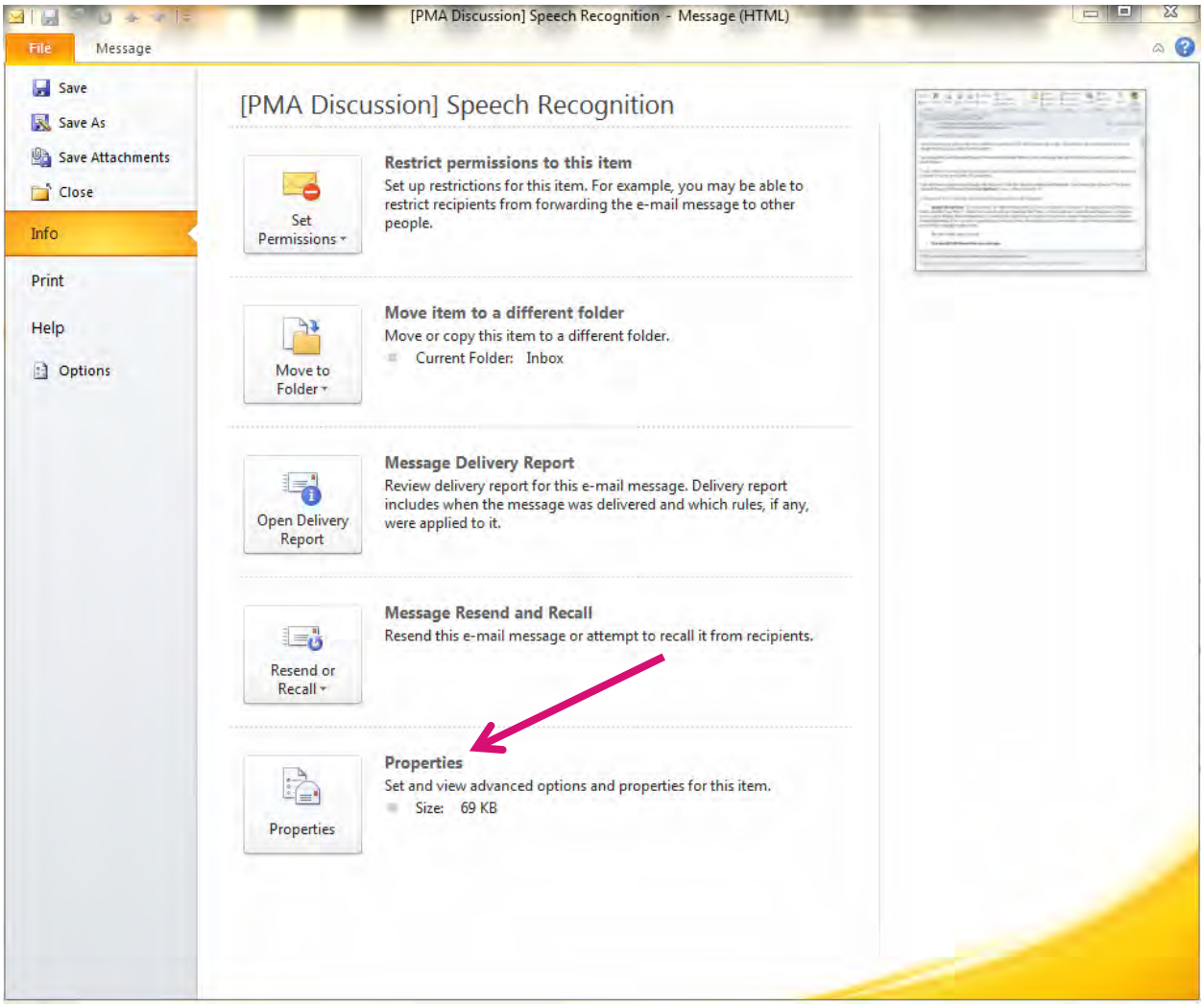
EMAIL

The date stamp of an email and the names attached to it are not obscure. Every email has a detailed background of metadata that tells where it was routed and how it is configured, as in example:



The internet headers for this email are three pages long, if you copied all of them.

To find the metadata, go to **File** and **Properties**.

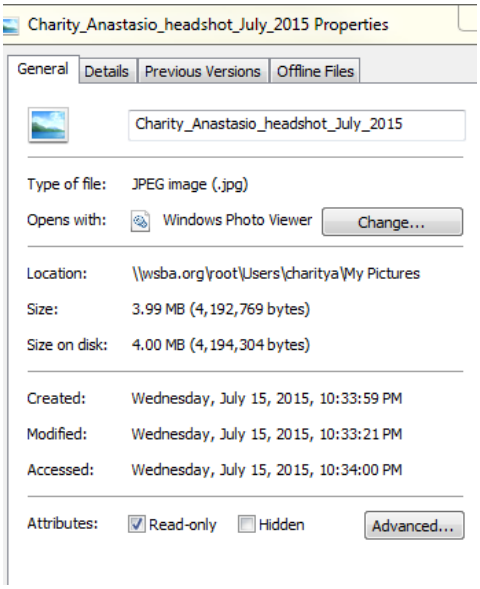


DIGITAL PHOTOGRAPHS AND VIDEOS

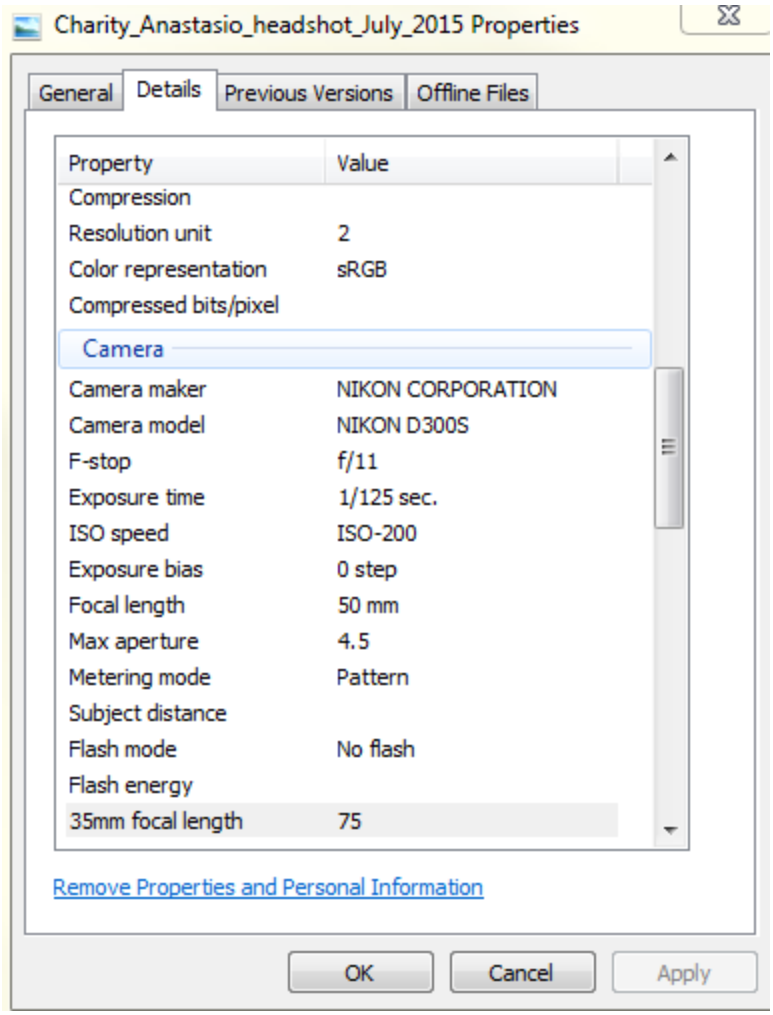
The information behind a picture or video in digital media tells much of the same information it tells in paper formats. Think of it as the red date stamp that used to appear on photographs with older cameras where that option could be turned on or off, but hidden in the background.

For example, digital pictures also contain metadata. Go to **File** and **Properties**:

Several tabs will open up, usually with the Details tab being the default. **General** offers size and location of the picture (where it is saved), including date stamps, title, and what kind of file:



Details may give author, programs used on it, more detailed size, camera make, model, exposure, F-stop used, and information on lenses used, among other things.



ADOBE ACROBAT X

Despite the fact that the PDF, or portable document format, conversion is one of the primary methods for stripping key metadata from a document, metadata lives in PDFs as well. There are three versions of Adobe: Reader, Standard, and Pro, as well as many iterations and an online version. Everyone has the Reader as it is free and comes with most devises or can be downloaded. It is mainly just for seeing and reading PDFs, as the name would imply.

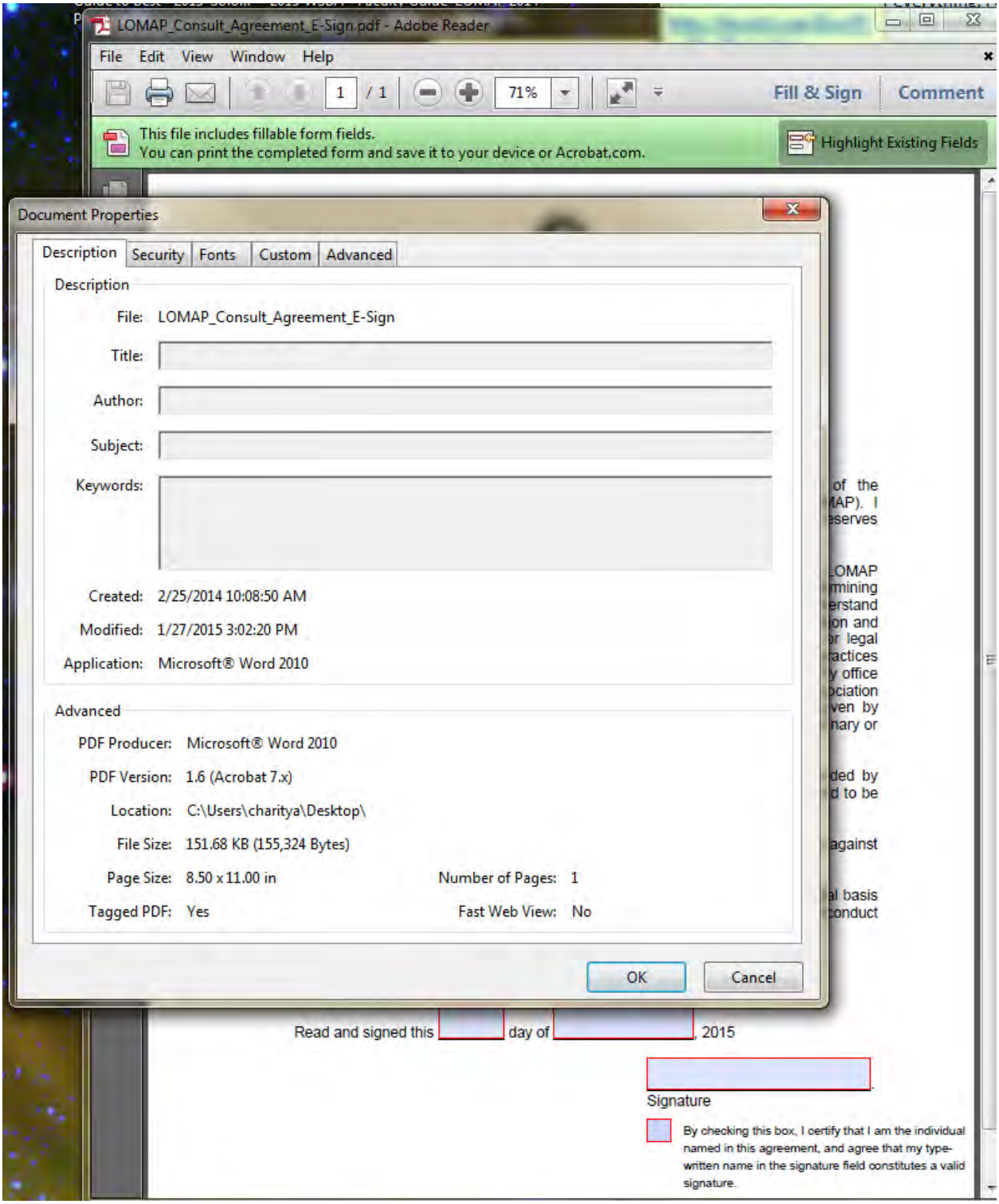
The Standard and Pro version have different features relevant to the stripping of harmful metadata. Below is a comparison chart of the different features, many of which may come into play (if one converts to another format, one needs to understand the metadata issues of that format, for example) and three of which will be discussed in more depth here because they are essential to the proper removal of harmful metadata (Actions in bold).

Action	Standard	Pro
Read PDF Files	x	x
Convert to Word or Excel files	x	x
Convert to PowerPoint		x
Convert PDF to HTML/web pages		x
Edit PDF files	x	x
Find and replace in PDFs	x	x
Merge files of different formats in PDF	x	x
Brand the merged file consistently		x
Insert audio, video, or interactive media		x
Create fillable forms in PDF	x	x
Advanced, easier PDF forms creation		x
Review and notate PDFs	x	x
Manage shared reviews		x
Compare two PDF versions and highlight	x	x
Sign document electronically	x	x
Get others' electronic signatures on PDFs	x	x
Protect and Restrict PDFs	x	x
Remove metadata	x	x
Redact information permanently		x
Create guided/automated steps to be applied to all PDFs created		x

Note that the standard version can "remove metadata" but one cannot create an automated system for the automatic removal of that data unless one uses a Pro version of Adobe Acrobat.

Although it is not technically metadata, it is important to note that sometimes lawyers will merely put black over information that must be redacted. That black can be easily removed to reveal the information behind it. So, if one must redact information on a PDF, it is essential to have the Pro version and to use the redaction tool that permanently redacts information in a PDF.

The metadata for a PDF lives in **Properties**, found under the **File** dropdown menu:


LOMAP_Consult_Agreement_E-Sign.pdf - Adobe Reader
File Edit View Window Help
1 / 1
71%
Fill & Sign
Comment
This file includes fillable form fields.
You can print the completed form and save it to your device or Acrobat.com.
Highlight Existing Fields
Document Properties
Description
Security
Fonts
Custom
Advanced
Description
File: LOMAP_Consult_Agreement_E-Sign
Title:
Author:
Subject:
Keywords:
Created: 2/25/2014 10:08:50 AM
Modified: 1/27/2015 3:02:20 PM
Application: Microsoft® Word 2010
Advanced
PDF Producer: Microsoft® Word 2010
PDF Version: 1.6 (Acrobat 7.x)
Location: C:\Users\charitya\Desktop\
File Size: 151.68 KB (155,324 Bytes)
Page Size: 8.50 x 11.00 in
Number of Pages: 1
Tagged PDF: Yes
Fast Web View: No
OK
Cancel
Read and signed this day of , 2015
Signature
By checking this box, I certify that I am the individual named in this agreement, and agree that my type-written name in the signature field constitutes a valid signature.

REMOVING METADATA

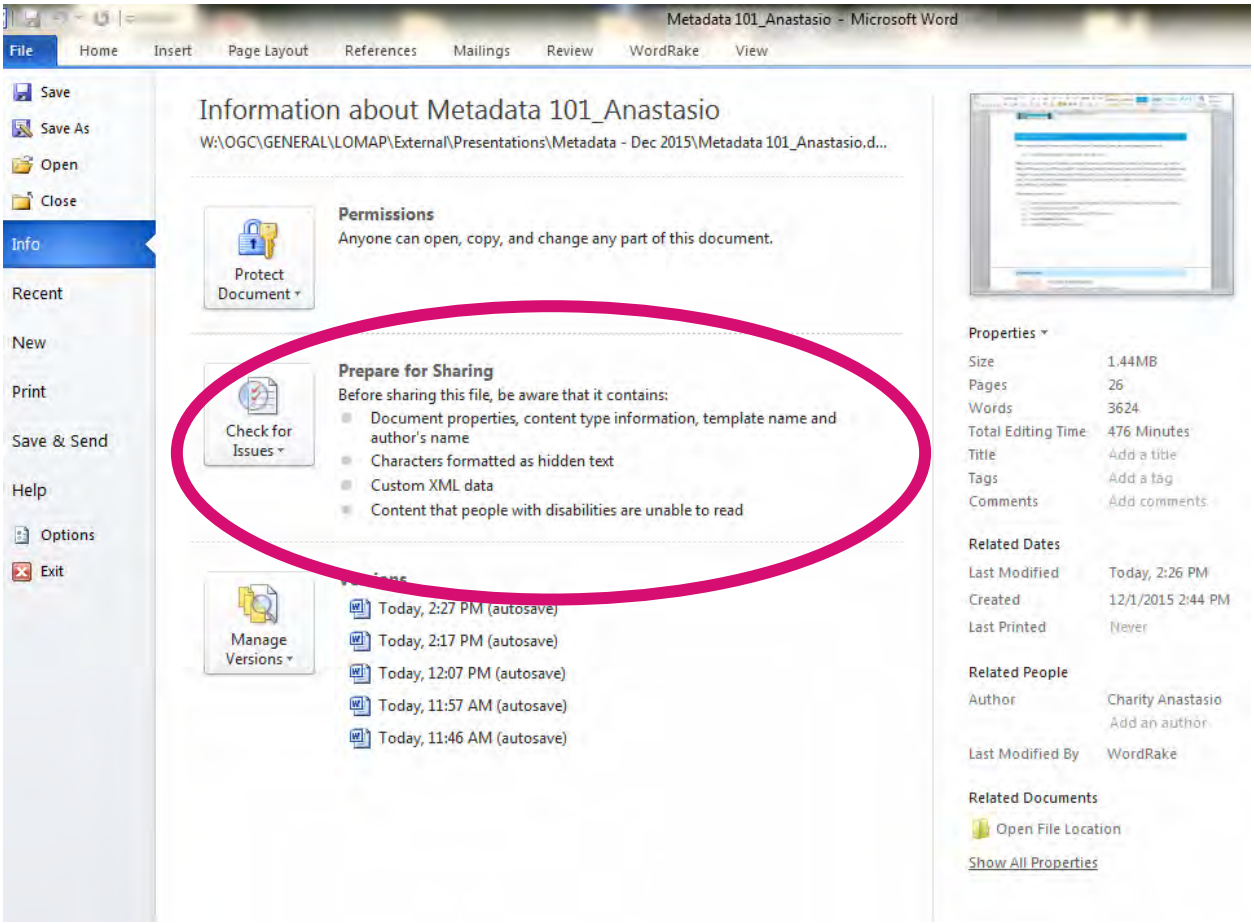
Now that you know where much of this secret data lives, here are some ways to remove it.

USE MICROSOFT PRODUCT INSPECTION AND REMOVAL TOOL

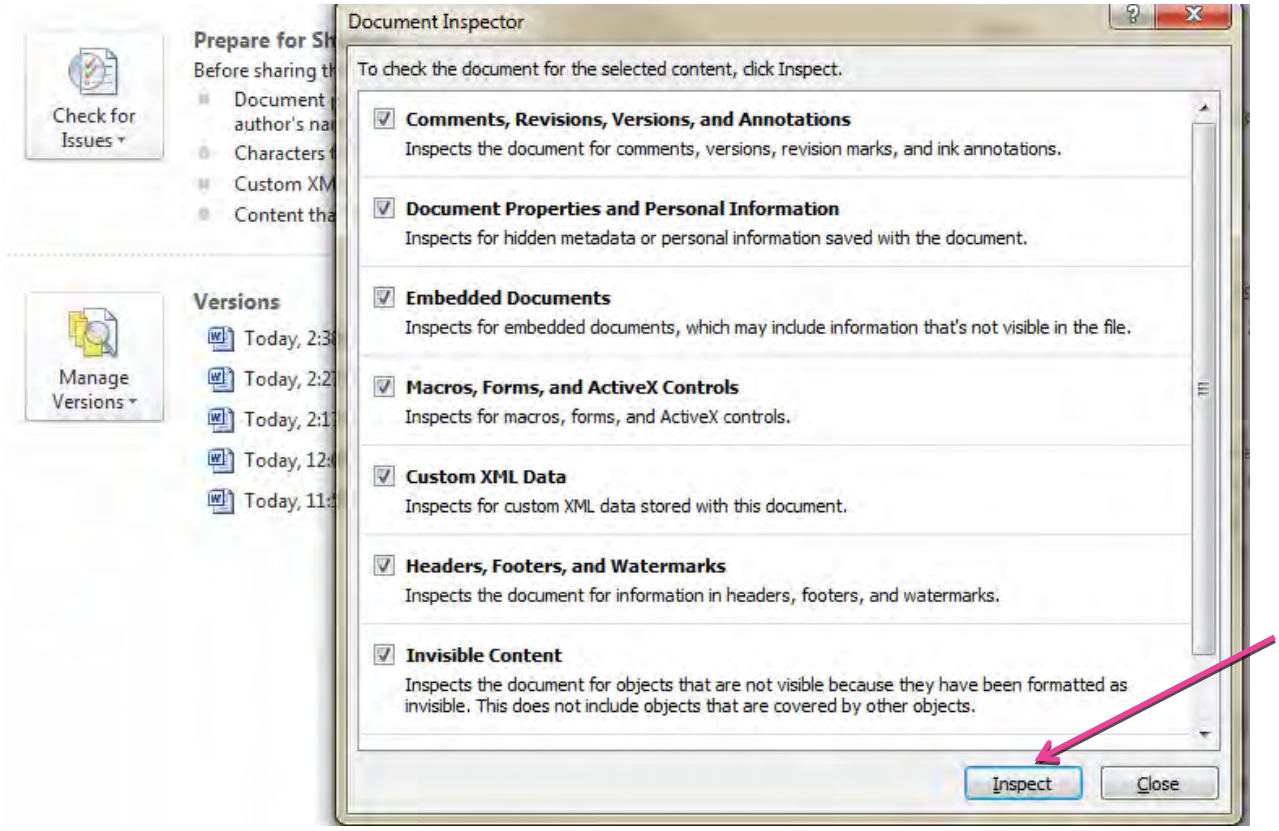
Microsoft 2000 and prior versions retained metadata on the last ten editors of a document, as well as other differences. By Office 2003/XP, removing hidden data was a free add-on that one could download, though it was somewhat untrusted. At this point, if you have an older version and open it with a newer one, some of that old metadata is automatically stripped off, but realize that the different versions may look different and feel different.

The version used here is Microsoft 2010.

Go to File →Information. Here is the metadata for this document. Know that the **Preparing to Share** section lists what data is present in this document before you even start, giving you a clue as to what you will be stripping out.

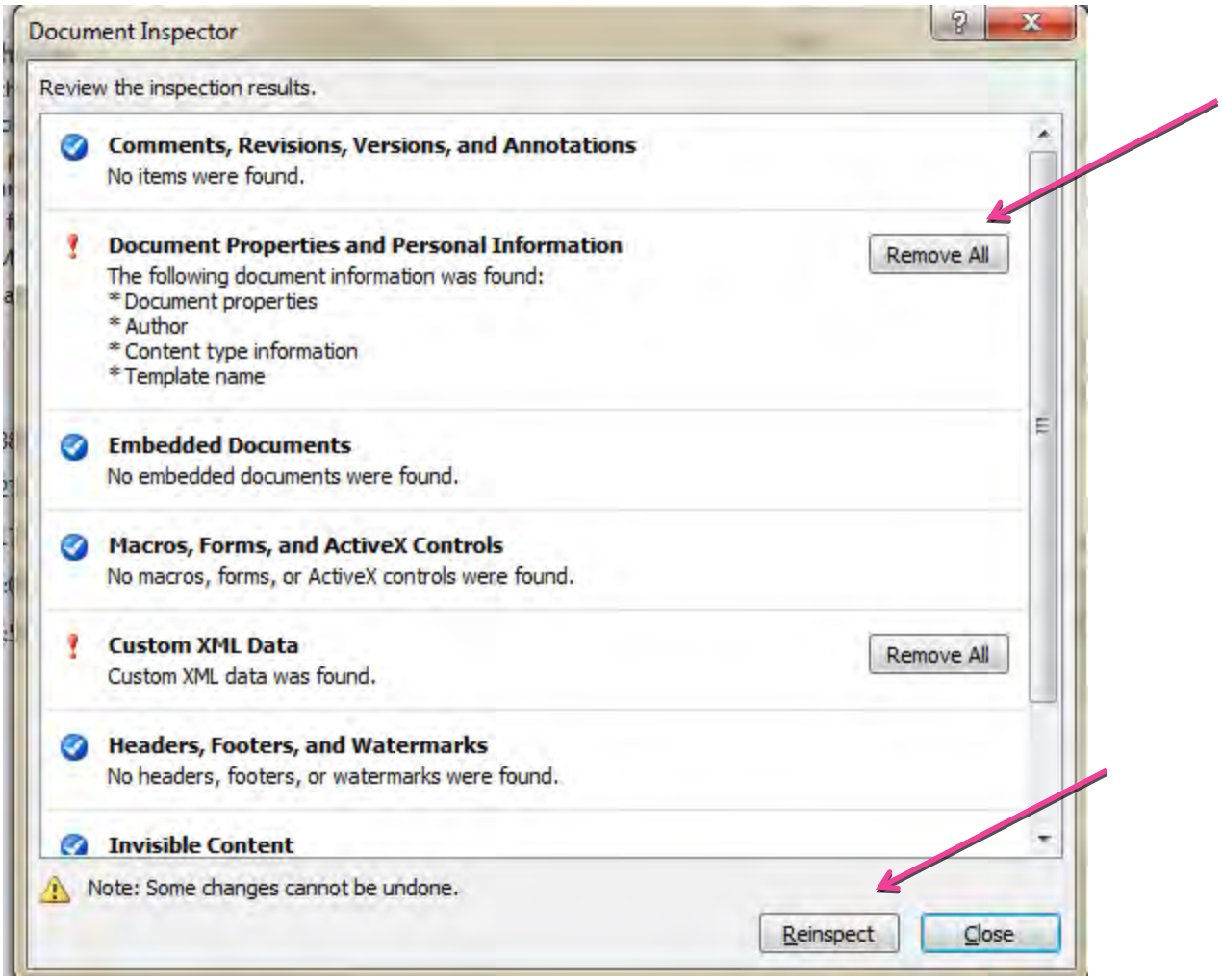


Click **Check for Issues**. It will give you a dropdown menu. The first thing listed is **Inspect Document**. Click this.

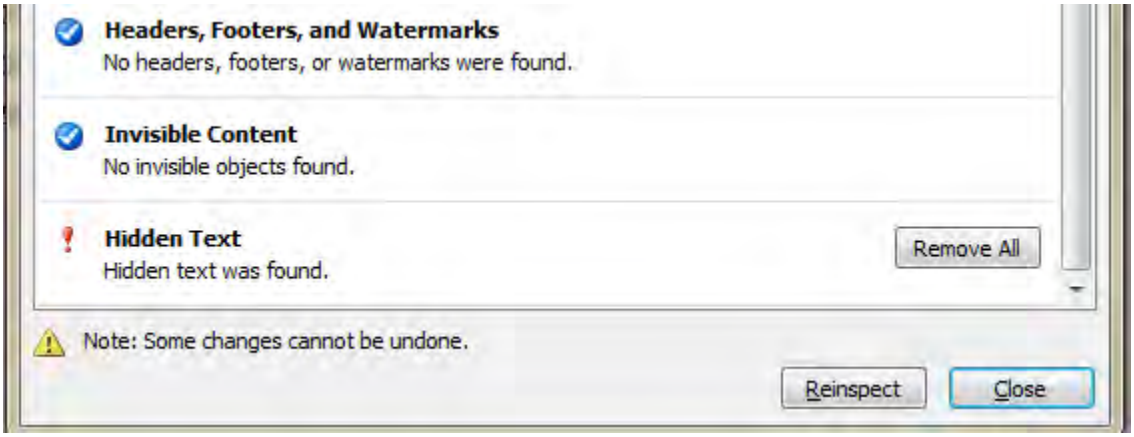


It will bring up all the issues it checks. It defaults to having them all checked, so uncheck things if you do not want to strip that metadata out.

Click **Inspect**. This document has several things that can be removed, including the classic metadata, custom XML data, and hidden text. Click **Remove All**.



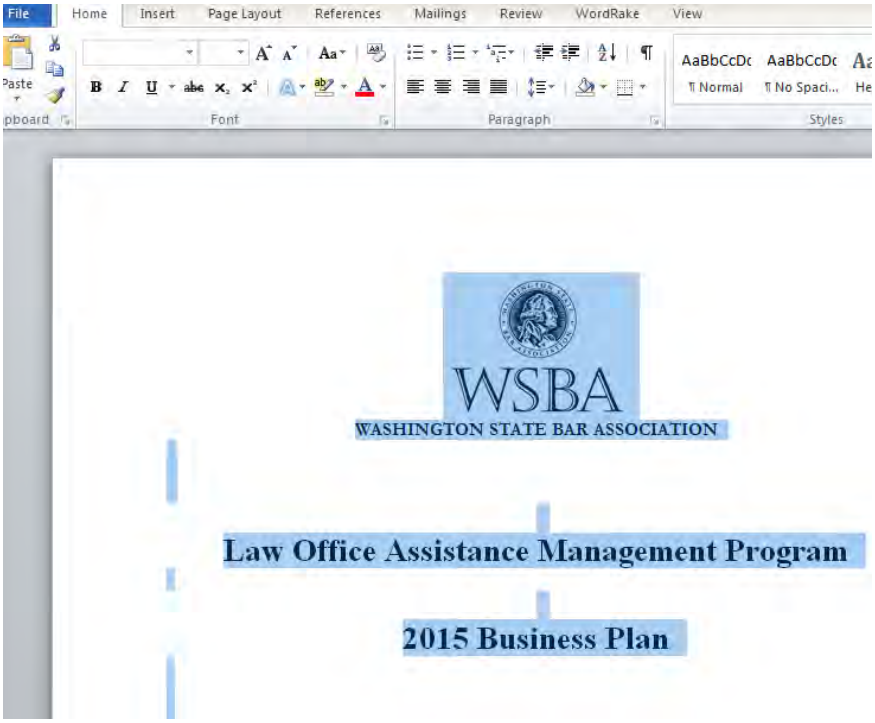
It should report that the information was removed. **Reinspect**. Most will be gone. If, as here, something cannot be undone, then determine if it is damaging or not to keep it.



CUT AND PASTE INTO A NEW DOCUMENT

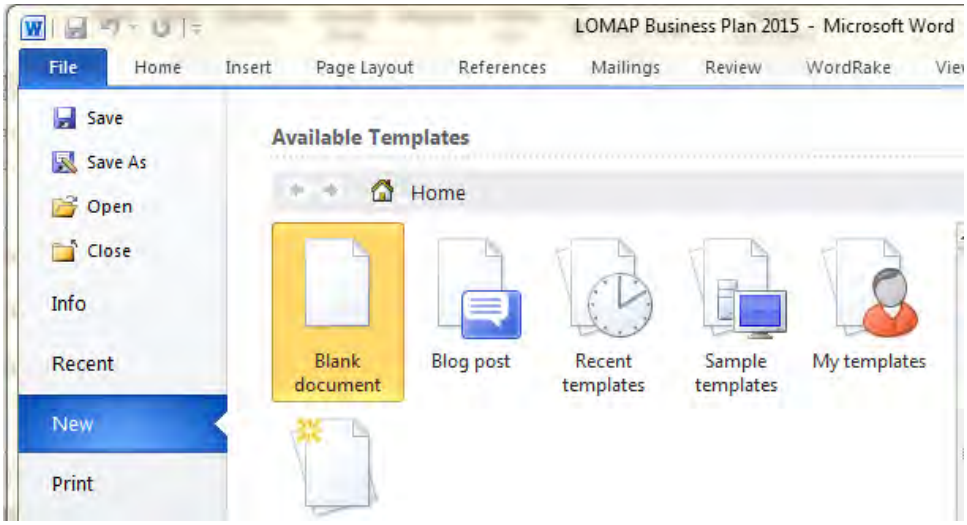
Create a new document and save everything from your former version into your new version

Another way to clean off metadata is to **Select All** (Cntrl +A), **Copy** (Cntrl +C), open a new blank document, and **Paste** (Cntrl +V).



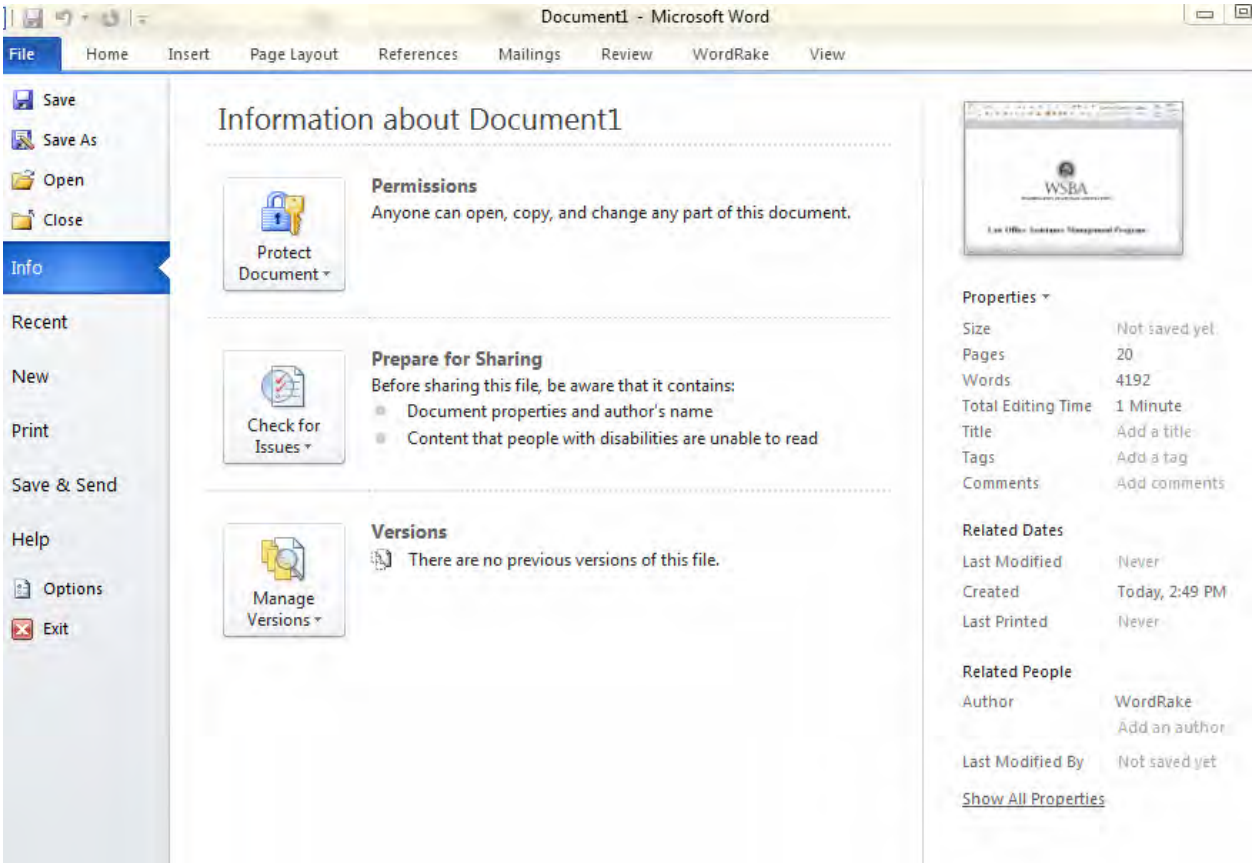
→

Select All (Cntrl +A) and **Copy** (Cntrl +C



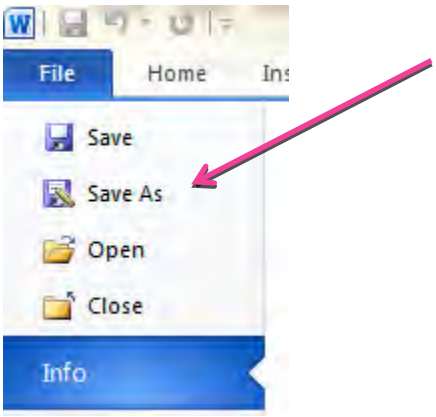
→

Open a new blank document, and **Paste** (Cntrl +V). See how the new properties has the correc pages and size, but the author is changed to what your computer is marked as and the time spent editing it is only one minute:

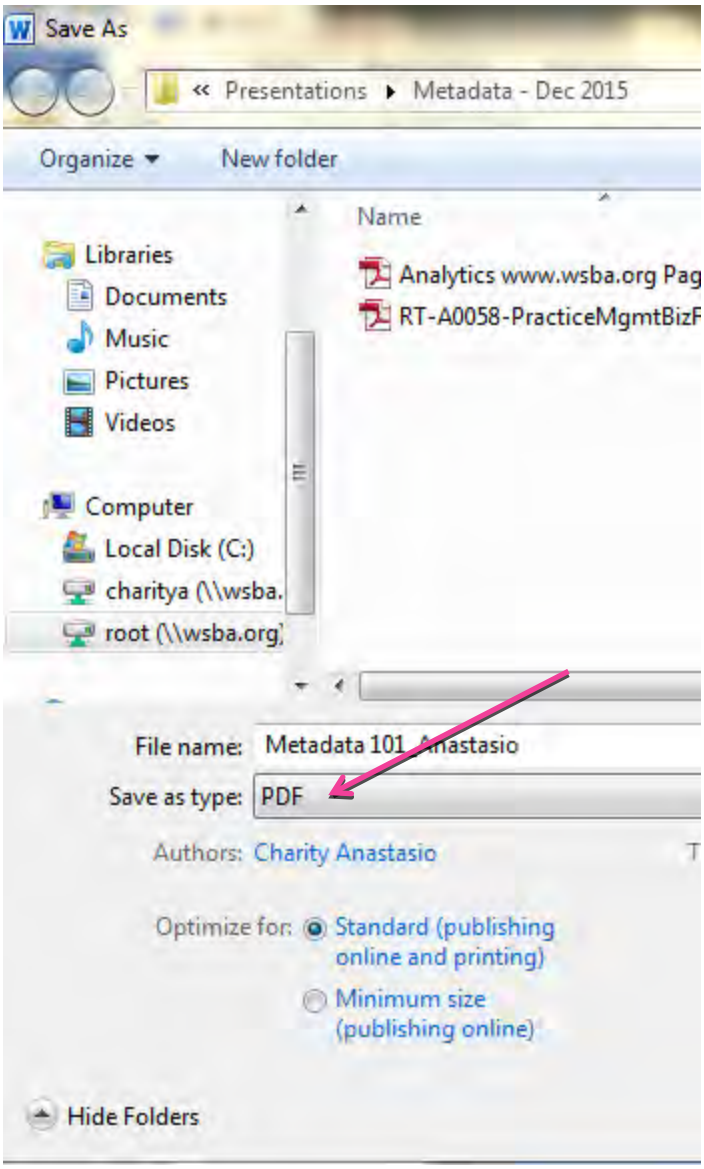


TURN THE DOCUMENT INTO A PDF

In the more recent versions of Microsoft products it is easy to turn a file into a PDF. Go to **File** and **Save As**.



A folder location will pop up in most versions. It will default to saving it as a Word document at the **Save as Type** field. Pull the drop down menu and select **PDF**.



If one has a version older than Microsoft Office 2007 or it is another product without a built in conversion, then it may require the use of a product like CutePDF or Adobe Acrobat to do the conversion. (It is recommended that one update software if using an older version than 2007.)

FAX OR SCAN AND SEND THE DOCUMENT (ALSO A PDF)

Use a scanner to scan a hardcopy of a document. Send this via email. It will have metadata, but only from the scanner, stamping the date and time it was scanned. Similarly, one could fax a copy of the document and it would have the fax tag, date and time stamp from the fax.

This is probably the most labor intensive method unless one is working in hardcopy already. The fax would result in someone needing to retype any edits, if it is a collaborative process. PDFs can be made

searchable through Adobe Acrobat (Optical Character Recognition or OCR), making searching for particular words or phrases easier. A PDF can also be edited, redlined, commented upon in Adobe Acrobat and similar products like Nuance PDF Creator. In the Pro version one can also disassemble and reassemble a PDF in a different order, so the collaborative process can carry on.

USE A METADATA SCRUBBER

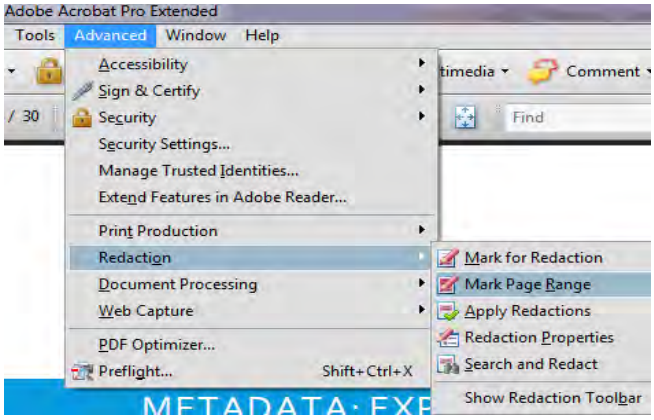
There are a number of metadata scrubbers out there. They all have free trials so that one can test them out:

- iScrub: http://esqinc.com/iscrub-trial/
- Doc Scrubber 1.2: http://doc-scrubber.en.softonic.com/
- Workshare: http://www.workshare.com/workshare/professional-9-in-action?utm_source=adwords&utm_medium=PPC&utm_campaign=SD-US-Brand&gclid=CLbsioqzzckCFYhBfgodHXIKbg
- PayneGroup: http://www.thepaynegroup.com/contact/?form=metadatatrial

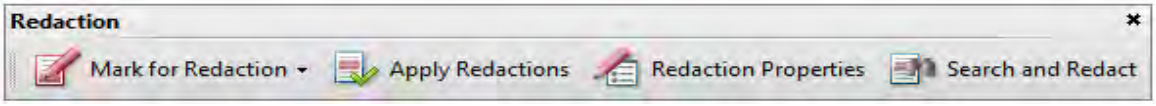
It is important to look for one that is visually and systematically appealing to the bulk of the users at the firm, that is instinctual and easy to use, is the right price point, but also syncs well with other products that are currently in use.

USE ADOBE ACROBAT PRO FUNCTIONS

Redaction. Adobe Acrobat comes in three versions: Reader (everyone has loaded on devises or downloadable for free), standard (some functionality, but not advanced level redaction appropriate for most law firms), and Pro (the right version for most law firms). Within these there are many different versions. Most of the secreenshots and instructions in these materials are for version X, but redaction exists in earlier versions as well. For example, Adobe Acrobat Pro 9 (which is not supported anymore and is a security risk to keep using) has the redaction menu under **Advanced → Redaction**.

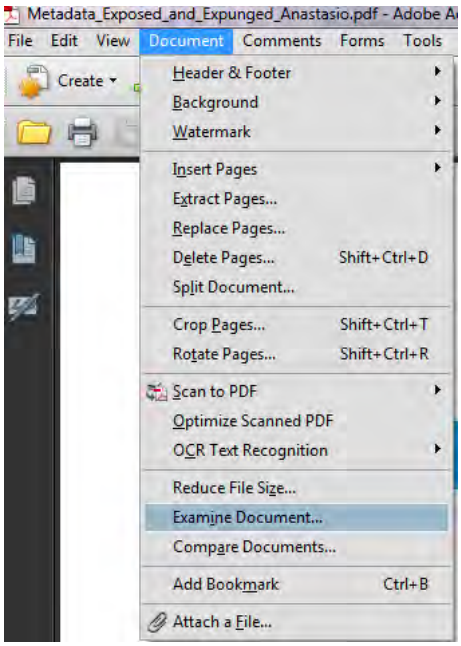


If one selects Show Redaction Toolbar, the functions are pulled out as such:

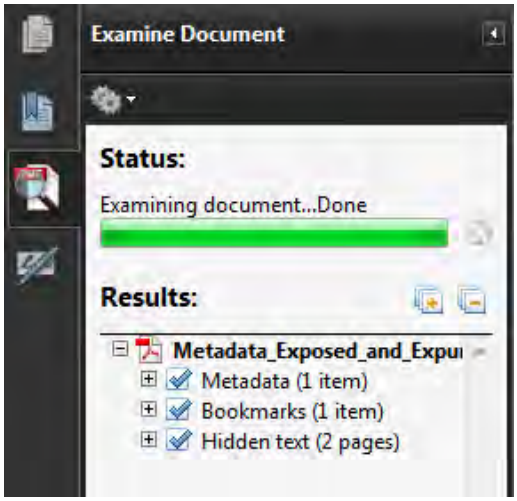


Start with Mark for Redaction to pick own information visually, or Search and Redact to find words, phrases, or numbers throughout the document.

Examine and Remove Metadata. Also in Adobe Acrobat , one can examine the metadata of a document under **Documents → Examine Document**.



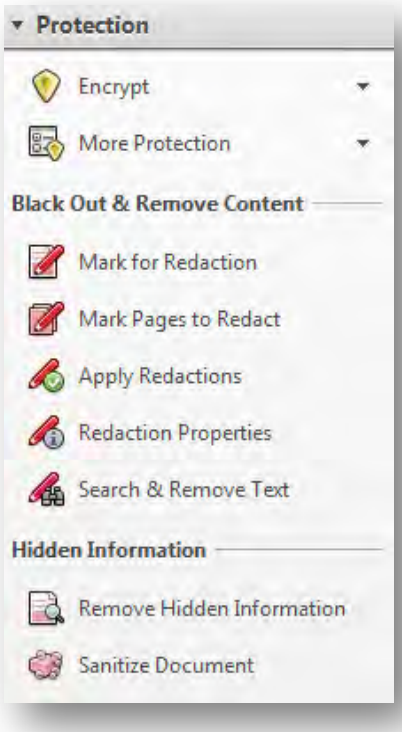
The program produces a report where all metadata is stored. Each one of these is clickable and will take one to the location of the metadata. Not all metadata is harmful or should be removed. Here, it is primarily the bookmarks for the table of contents, something most would decide to maintain instead of stripping out.

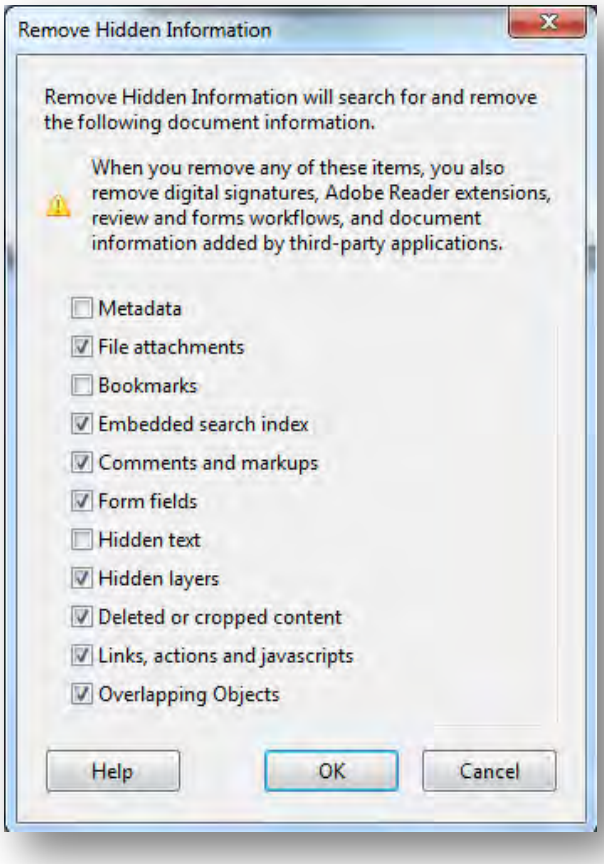


Automation. (These instructions are for a later version of Adobe Acrobat Pro.) Create an automated workflow that includes such things as redaction and the creation and cleaning off the metadata every time a document is prepared in Adobe Acrobat.

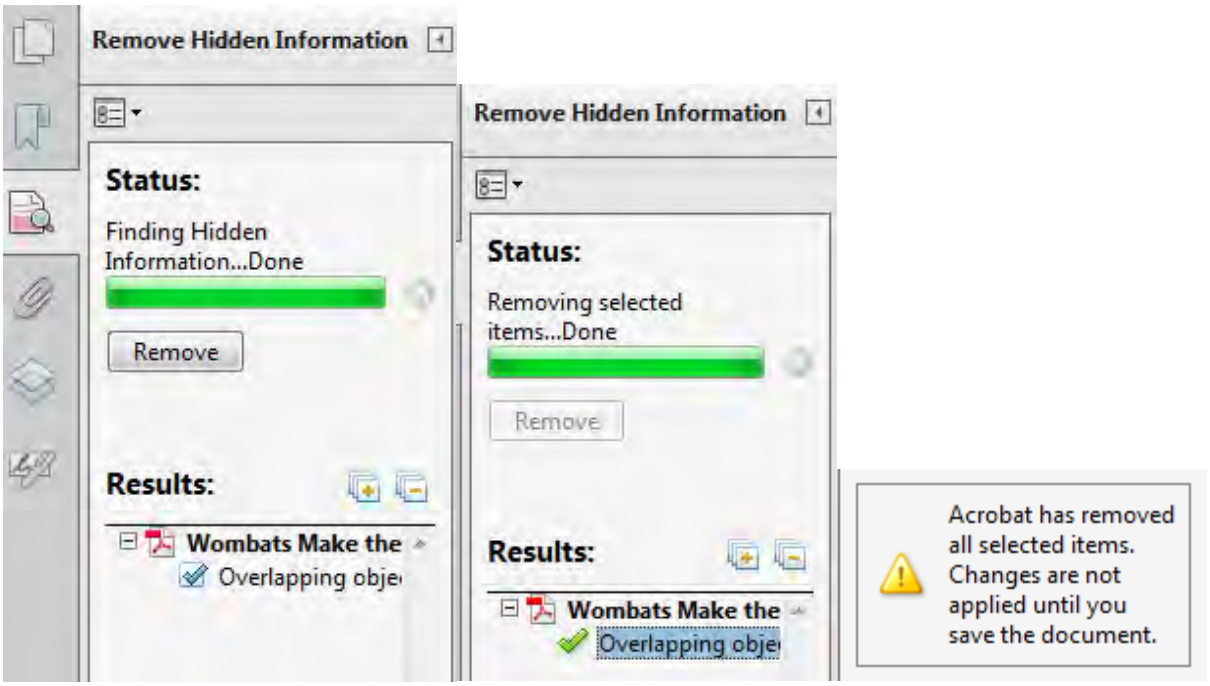
Go to **Tools → Protection → Hidden Information**.

Click on **Remove Hidden Information** and a pane pops up that tells you what will be removed.

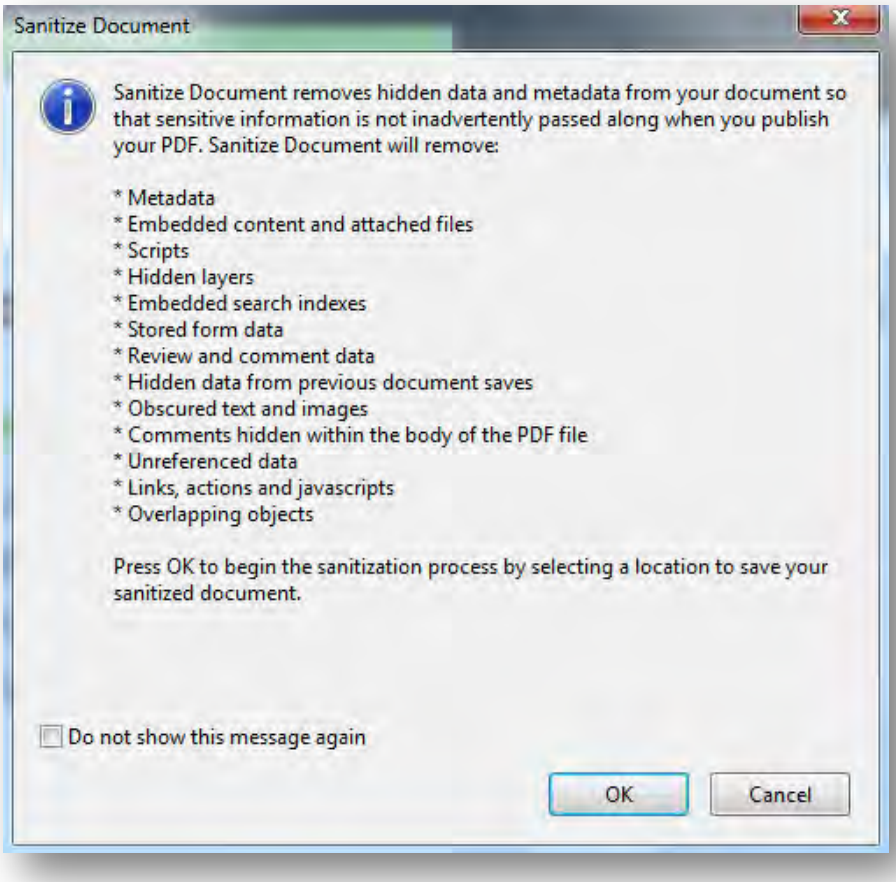




Adobe will give you a report of the hidden data. Click **Remove** and it will remove it and inform you after the task is complete. (See below.)



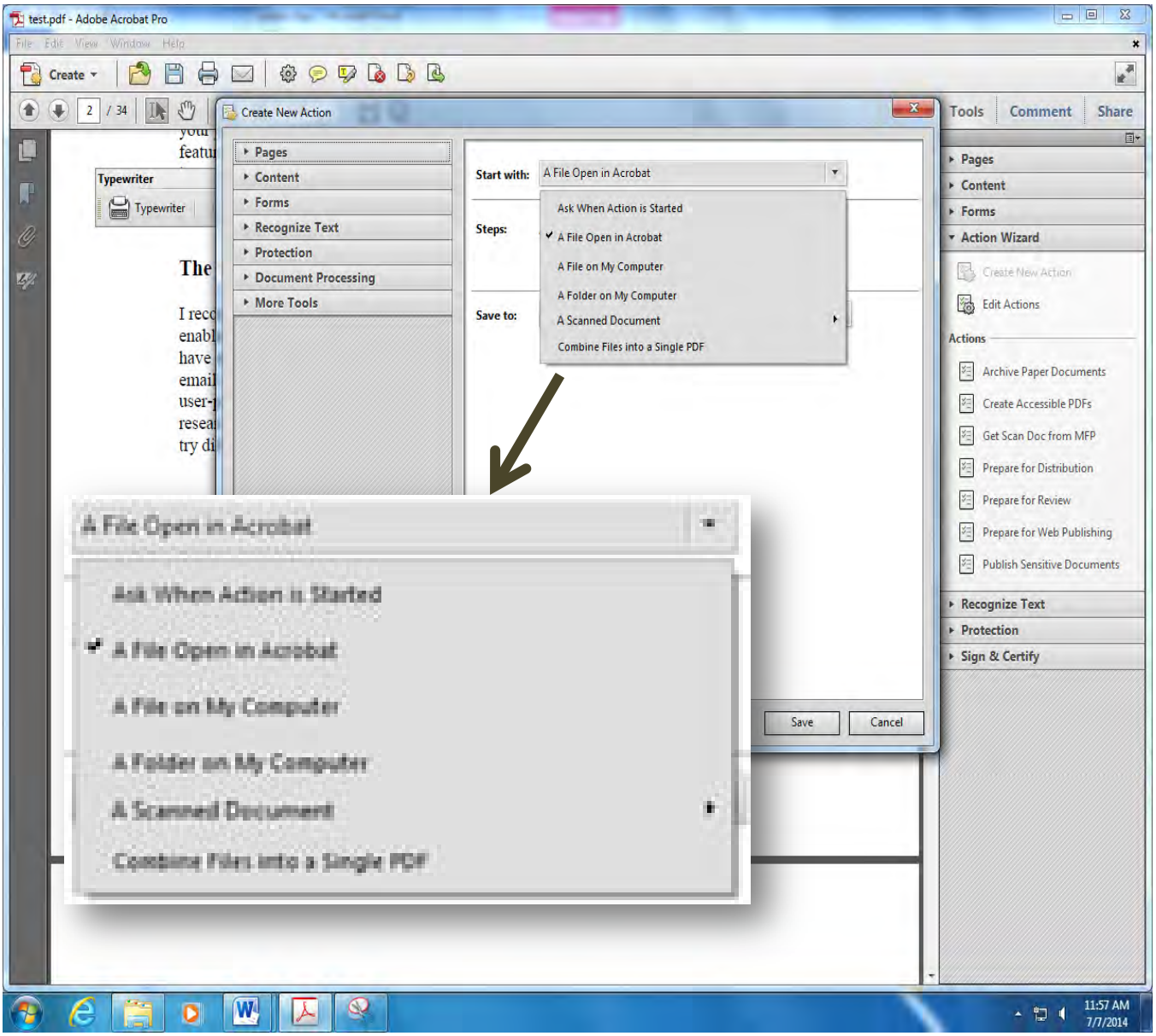
Hidden Information removal is customizable, permitting you to select what data you wish to retain. **Sanitize Document** will do just that, removing all the items on the list below.



Using Action Wizards to Save Time

Action Wizard sets up a series of actions that will happen automatically or prompt the author to do them automatically. This is a huge efficiency enhancement of Adobe. It is only available in Adobe Pro. This permits the editor to set up a series of tasks associated with a certain type of PDF, or all PDFs that will standardize the branding of the firm and simplify training, because Adobe can prompt the drafter to do them before saving. Think of it as a checklist of procedures to finish a document properly.

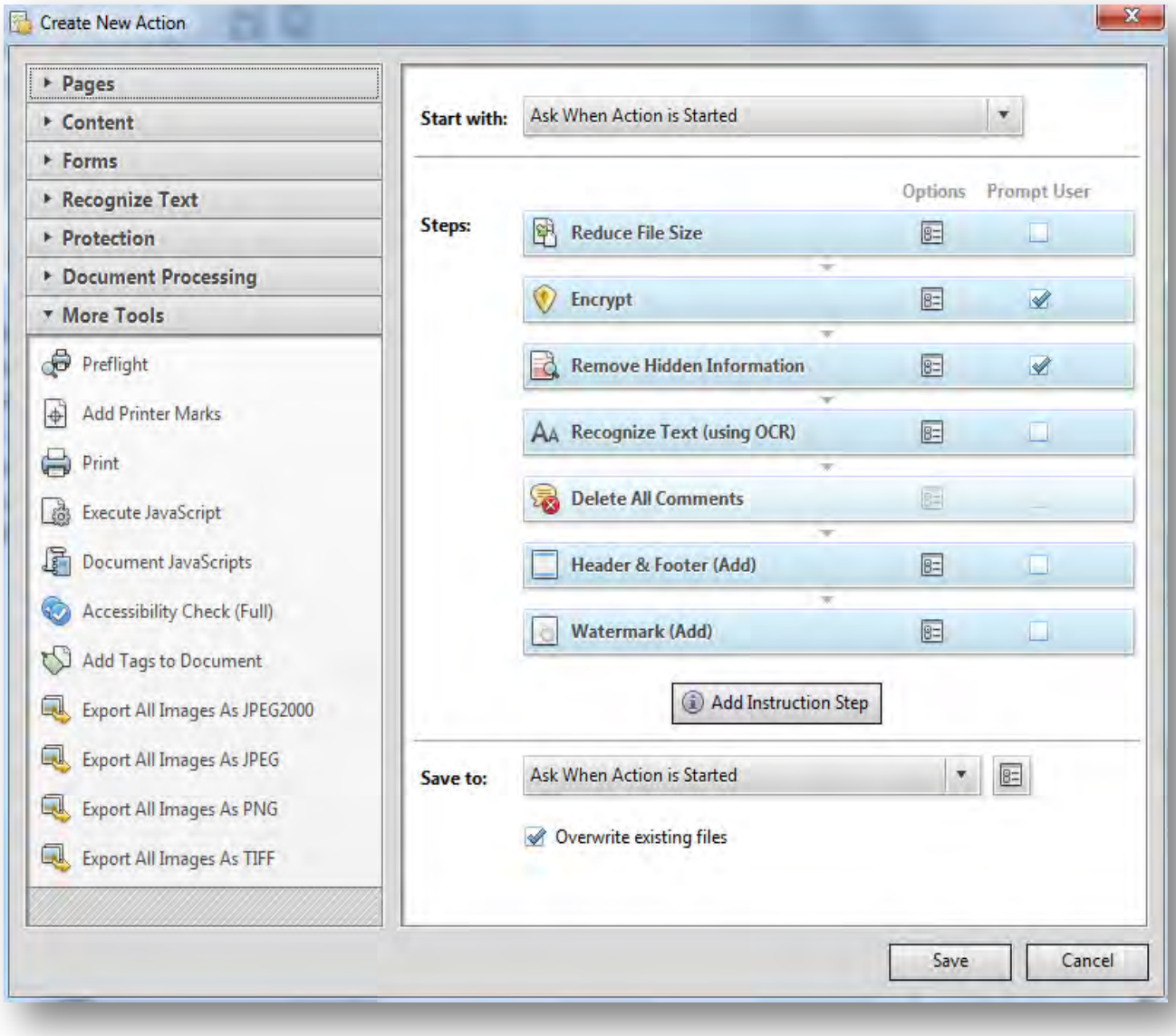
Go to **Tools→ Action Wizard → Create New Action**. Determine when the series of actions will be taken.



Click on the actions you wish to make up the series. For example, here (below) I selected encryption, delete comments, remove hidden information (metadata), and reduce the file size, because this PDF is

being prepared to be shared with opposing counsel and has client confidential information on it. I add a Watermark because it is a draft and a header and footer to brand it to the firm's look. I select recognize text using OCR which means that it will be a searchable PDF.

These steps should be customized to your policies and procedures.



What is most important is that this becomes a standard that the entire firm employs with every outside bound document. The new procedure should be

- Researched and the change planned
- written up
- placed in the procedures and policies manual once it is approved
- communicated to the staff

- trained on initially and then repeated or revisited at regular intervals, and
- followed religiously from top to bottom.

If it is not, then best laid plans are for naught.

With careful protocols and systems you can ensure confidential information and legal strategy will not be inappropriately disclosed to opposing counsel, the courts or the public. It is an ethical duty to protect such information, so hone those redaction and metadata stripping skills and be inquisitive. Ask whether the document or other media you are sending out says anything you do not want it to say, whether on its face or not, before sending it out.

RESOURCES

Beware the Dangers of Metadata, Dan Pinnington, LAWPRO Magazine, June 2004.

Document Metadata: What You Can't See Can Actually Hurt You, by Workshare, 2015.

Metadata Ethics Opinions, ABA.

Metadata: The Ghosts Haunting e-Documents, David Hricik and Chase Edward Scott, Georgia Bar Journal, February 2008, p. 16 - 24.

Metadata: What It Is and Why You Should Care, Susan J. Silvernail, Alabama Association for Justice, August 11, 2007

The New Metadata Rules, Donna Payne, International Legal Technology Association, October 2008.

What's the Matter With Metadata?, Charles F. Luce, Jr., Technology In The Law Practice, 2007.

119 DISCLOSURE, REVIEW, AND USE OF METADATA

Adopted May 17, 2008.

Introduction

Lawyers routinely send and receive documents or computer files in electronic form, whether in email correspondence, in the course of civil discovery, or otherwise. An electronic document typically includes data that may or may not be visible when viewing the document on the computer screen or as printed out. These hidden data are called "metadata." Metadata embedded in a document can include such information as the dates and times that the document was created, modified, and accessed, and the names of the persons who created the document and who last edited the document. Metadata can also include embedded user comments or the edit history of a document, including redlined changes showing additions and deletions of text. Metadata in spreadsheets include the formulas used to arrive at the numbers displayed in a table. This list of types of metadata is not complete. Moreover, common types of metadata are likely to change and multiply over time as computer software and technology change.

Much metadata is of little or no practical significance. For example, it may be of no importance when a document was created and edited or by whom. Other metadata, such as formulas in a spreadsheet, may be important but not confidential. Some metadata, however, particularly metadata such as hidden comments or redlines, can be Confidential Information. "Confidential Information" is used in this Opinion to include information that is subject to a legally recognized exemption from discovery and use in a civil, criminal, or administrative action or proceeding, even if it is not "privileged." *See* Op. 108.

This opinion addresses the ethical obligations of a lawyer (the "Sending Lawyer") who transmits electronic documents containing metadata to a third party, including the lawyer for an adverse party. This opinion also addresses the ethical obligations of a lawyer (the "Receiving Lawyer") who receives electronic documents containing metadata from a third party, including the lawyer for an adverse party or a non-lawyer third party.

Syllabus

A Sending Lawyer who transmits electronic documents or files has a duty to use reasonable care to guard against the disclosure of metadata containing Confidential Information. What constitutes reasonable care will depend on the facts and circumstances. The duty to provide competent representation requires a Sending Lawyer to ensure that he or she is reasonably informed about the types of metadata that may be included in an electronic document or file and the steps that can be taken to remove metadata if necessary. Within a law firm, a supervising lawyer has a duty to ensure that appropriate systems are in place so that the supervising lawyer, any subordinate lawyers, and any nonlawyer assistants are able to control the transmission of metadata.

A Receiving Lawyer who receives electronic documents or files generally may search for and review metadata. If a Receiving Lawyer knows or reasonably should know that the metadata contain or constitute Confidential Information, the Receiving Lawyer should assume that the Confidential Information was transmitted inadvertently, unless the Receiving Lawyer knows that confidentiality has been waived. The Receiving Lawyer must promptly notify the Sending Lawyer. Once the Receiving Lawyer has notified the Sending Lawyer, the lawyers may, as a matter of professionalism, discuss whether a waiver of privilege or confidentiality has occurred. In some instances, the lawyers may be able to agree on how to handle the matter. If this is not possible, then the Sending Lawyer or the Receiving Lawyer may seek a determination from a court or other tribunal as to the proper disposition of the electronic documents or files, based on the substantive law of waiver.

If, before examining metadata in an electronic document or file, the Receiving Lawyer receives notice from the sender that Confidential Information was inadvertently included in metadata in that electronic document or file, the Receiving Lawyer must not examine the metadata and must abide by the sender's instructions regarding the disposition of the metadata.

Opinion

Metadata are not really different from any other sort of information. In Formal Opinion 108, the Committee addressed a lawyer's obligations with respect to receipt of inadvertently transmitted documents. In Formal Opinion 90, the Committee addressed a lawyer's obligations to be aware of disclosure of Confidential Information using new technology. In most respects, this opinion is an application of those two previous opinions and the underlying Rules. The Committee believes that this separate opinion regarding metadata is appropriate because there is a split among other jurisdictions over the application of familiar rules to a type of data that is new and mysterious to some.

1. The Sending Lawyer's Obligations to Guard Against Disclosure of Metadata Containing Confidential Information.

Under the Colorado Rules of Professional Conduct, a Sending Lawyer has an ethical duty to take steps to reduce the likelihood that metadata containing Confidential Information would be included in an electronic document transmitted to a third party. This duty arises out of several interrelated rules.

First, Rule 1.6(a) provides that "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is [otherwise] permitted. . . ." Second, Rule 1.1 provides that "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." Third, Rules 5.1 and 5.3 generally require a lawyer to make reasonable efforts to ensure that the lawyer's firm, including lawyers and non-lawyers, conform to the Rules.

Under these Rules, a Sending Lawyer must act competently to avoid revealing a client's Confidential Information, and to ensure that others at the Sending Lawyer's firm similarly avoid revealing a client's Confidential Information. This requires a Sending Lawyer to use reasonable care to ensure that metadata that contain Confidential Information are not disclosed to a third party. *See* DC Ethics Op. 341 (2007); Maryland State Bar Ass'n Formal Ethics Op. 2007-09, "Ethics of Viewing and/or Using Metadata," ("the sending attorney has an ethical obligation to take reasonable measures to avoid the disclosure of confidential or work product materials imbedded in the electronic discovery"); Arizona Ethics Op. 07-03, "Confidentiality; Electronic Communications; Inadvertent Disclosure" (same); Alabama Ethics Op. RO-2007-02, "Disclosure and Mining of Metadata" (same); Florida Ethics Op. 06-2 (same); New York State Bar Ass'n Comm. on Prof'l Ethics, Op. 782 (2004) (same); *see also* CBA Formal Ethics Op. 90, "Preservation of Client Confidences in View of Modern Communications Technology" (1992) ("A lawyer must exercise reasonable care when selecting and using communications devices in order to protect the client's confidences or secrets from unintended disclosure.").

What constitutes reasonable care will depend on the facts and circumstances. For example, a Sending Lawyer could avoid creating certain types of metadata by choosing not to use redlining or hidden comments in a document that may be transmitted to third parties. In addition, software is available to "scrub" files of some types of metadata. In a circumstance where it is vital that no metadata be transmitted, a Sending Lawyer could print out an electronic document to ensure absolutely that no unseen metadata of any kind are included. Other methods of controlling or preventing disclosure of metadata exist.[1]

In many instances, it would be appropriate for a lawyer to retain persons with expertise in computer software and hardware, either through an in-house computer systems department in a larger firm, or through outside contract vendors for a smaller firm or solo practice. These computer experts can set up systems to control or prevent the transmission of metadata.

A supervising lawyer has a duty to make reasonable efforts to make sure that the lawyer's firm has appropriate technology and systems in place so that subordinate lawyers and nonlawyer assistants can control transmission of metadata. RPC 5.1; RPC 5.3.

The ultimate responsibility for control of metadata rests with the Sending Lawyer. A Sending Lawyer may not limit the duty to exercise reasonable care in preventing the transmission of metadata that contain Confidential Information by remaining ignorant of technology relating to metadata or failing to obtain competent computer support. The duty to provide competent representation requires a lawyer to ensure that he or she is rea-

sonably informed about the types of metadata that may be included in an electronic document or file and the steps that can be taken to remove metadata. *See* DC Ethics Op. 341 (2007) ("lawyers must either acquire sufficient understanding of the software that they use or ensure that their office employs safeguards to minimize the risk of inadvertent disclosures"); New York State Bar Ass'n Comm. on Prof'l Ethics, Op. 782 (2004) (same).

2. The Receiving Lawyer's Obligations Upon Receiving Metadata

There are two distinct issues relating to a Receiving Lawyer's obligations regarding metadata. The first issue is whether the Receiving Lawyer ethically may review metadata. The second issue is what a Receiving Lawyer must do when he or she receives metadata that appear to contain Confidential Information.

a. May a Receiving Lawyer Ethically Review Metadata?

The authorities are split on whether a Receiving Lawyer ethically may review metadata in electronic documents received from adversaries or other third parties. The American Bar Association Ethics Committee concluded that the Model Rules of Professional Conduct generally do not prohibit a lawyer from searching for or reviewing embedded metadata in electronic documents or files received from opposing counsel, an adverse party, or other third party. ABA Formal Op. 06-442, "Review and Use of Metadata." The Maryland State Bar Association Ethics Committee followed the ABA on this point. Maryland State Bar Ass'n Formal Ethics Op. 2007-09, "Ethics of Viewing and/or Using Metadata." The District of Columbia Bar Association concluded that a Receiving Lawyer generally may review metadata included in an electronic document unless the Receiving Lawyer has actual knowledge that metadata containing Confidential Information were transmitted inadvertently. DC Ethics Op. 341 (2007).

The New York State Bar Association Committee on Professional Ethics concluded that a lawyer may not search for or review metadata in electronic documents received from third parties. The New York Committee stated that "A lawyer may not make use of computer software to surreptitiously 'get behind' visible documents." New York State Bar Ass'n Comm. on Prof'l Ethics, Op. 749 (2001). The New York opinion relied on a lawyer's ethical obligation under the New York Code of Professional Responsibility to refrain from dishonest, fraudulent, or deceitful conduct. New York's lead was followed by the bar association ethics committees of Arizona, Alabama, and Florida.[2] Arizona Ethics Op. 07-03, "Confidentiality; Electronic Communications; Inadvertent Disclosure"; Alabama Ethics Op. RO-2007-02, "Disclosure and Mining of Metadata"; Florida Ethics Op. 06-2; *see also* D. Hricik, *Mining for Embedded Data: Is It Ethical to Take Intentional Advantage of Other People's Failures?*, *N.Car. J. of Law & Tech.* 231 (Spring 2007) (reaching the same conclusion). The Alabama decision relied on Alabama's version of Colorado Rule of Professional Conduct 8.4 which prohibits "conduct involving dishonesty, fraud, deceit, or misrepresentation." These opinions—as evidenced by their use of such language as "mining"—appear to be based on an implied premise that searching for metadata is surreptitious or otherwise involves procedures that are difficult or complicated. They also seem to assume that metadata generally contain Confidential Information and that any metadata transmitted to a third party must, therefore, have been transmitted inadvertently.

The Committee concludes that the ABA, Maryland, and District of Columbia opinions are better reasoned, and that the New York, Arizona, Alabama, and Florida opinions are based on incorrect factual premises regarding the nature of metadata. Thus, the Committee concludes that a Receiving Lawyer generally may ethically search for and review metadata embedded in an electronic document that the Receiving Lawyer receives from opposing counsel or other third party. This conclusion is supported by the following.

First, there is nothing inherently deceitful or surreptitious about searching for metadata. Some metadata can be revealed by simply passing a computer cursor over a document on the screen or right-clicking on a computer mouse to open a drop-down menu that includes the option to review certain metadata. Typical word processing software can be configured so that files are routinely opened to show redlines or embedded comments.[3] Referring to searching for metadata as "mining" or "surreptitiously 'get[ting] behind'" a document is, therefore, misleading.

Second, an absolute ethical bar on even reviewing metadata ignores the fact that, in many circumstances, metadata do not contain Confidential Information. To the contrary, in some circumstances metadata are

intended to be searched for, reviewed, and used. For example, in discovery in a civil case, a party is entitled to discover pre-existing files in electronic form to enable review of metadata to trace the history of a document, its authors, edits, and comments. *See, e.g.,* Fed. R. Civ. P. 34 (explicitly requiring production of electronically stored information). As another example, when opposing parties are negotiating a document, a Sending Lawyer may specifically intend a Receiving Lawyer to review some metadata, such as redlines or comments in a draft of the document. Similarly, when a Sending Lawyer transmits a spreadsheet, the Sending Lawyer may intend that the Receiving Lawyer be able to see the formulas used in the spreadsheet so that the Reviewing Lawyer may understand and rely upon the numbers in the rows and columns of the spreadsheet.

Third, metadata are often of no import. In many circumstances it is of no significance who created a document, when the document was created, or the like.

Once one discards the notions that it is dishonest or deceitful to search for or look at metadata or that metadata typically contain significant Confidential Information, there is no Rule in the Colorado Rules of Professional Conduct that contains any prohibition on a lawyer generally reviewing or using information received from opposing counsel or other third party. Therefore, a Receiving Lawyer generally may search for and review any metadata included in an electronic document or file.

b. The Receiving Lawyer's Obligations On Discovering that He or She Has Received Metadata that Appear to Contain Confidential Information.

If a Receiving Lawyer knows or reasonably should know that a Sending Lawyer (or non-lawyer) has transmitted metadata that contain Confidential Information, the Receiving Lawyer should assume that the Confidential Information was transmitted inadvertently, unless the Receiving Lawyer knows that confidentiality has been waived. The Receiving Lawyer must promptly notify the Sending Lawyer (or non-lawyer sender). Once the Receiving Lawyer has notified the Sending Lawyer, the lawyers may, as a matter of professionalism, discuss whether a waiver of privilege or confidentiality has occurred. In some instances, the lawyers may be able to agree on how to handle the matter. If this is not possible, then the Sending Lawyer or the Receiving Lawyer may seek a determination from a court or other tribunal as to the proper disposition of the electronic documents or files, based on the substantive law of waiver.

If, before examining metadata in an electronic document or file, the Receiving Lawyer receives notice from the sender that Confidential Information was inadvertently included in metadata in that electronic document or file, then the analysis changes. In this scenario, the Receiving Lawyer must not examine the metadata and must abide by the Sending Lawyer's instructions regarding the disposition of the metadata.

We reach these conclusions as follows.

It is reasonable to expect that a Sending Lawyer will seek to act competently (under Rule 1.1) to protect the Confidential Information of the Sending Lawyer's client (under Rule 1.6). Accordingly, it is reasonable to assume that the Sending Lawyer would not intentionally transmit to opposing counsel or another third party any Confidential Information included in metadata in an electronic document or file. Thus, a Receiving Lawyer reasonably should believe that any Confidential Information contained in metadata received from the Sending Lawyer was transmitted inadvertently.

Because the Receiving Lawyer reasonably should believe that Confidential Information in metadata was transmitted inadvertently, Rule 4.4(b) is directly applicable. Rule 4.4 provides:

Rule 4.4. Respect for Rights of Third Persons

(a) In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person.

(b) A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.

(c) Unless otherwise permitted by court order, a lawyer who receives a document relating to the representation of the lawyer's client and who, before reviewing the document, receives notice

> from the sender that the document was inadvertently sent, shall not examine the document and shall abide by the sender's instructions as to its disposition.

Under Rule 4.4(b), once a Receiving Lawyer knows or reasonably should know that an electronic document or file contains metadata that appear to contain Confidential Information, the Receiving Lawyer should assume that the Confidential Information was transmitted inadvertently and must promptly notify the Sending Lawyer.[4] *See also* CBA Formal Ethics Op. 108, "Inadvertent Disclosure of Privileged or Confidential Documents" (2000).

Rule 4.4(b) does not state what the Receiving Lawyer should do after giving notice to the Sending Lawyer. May the Receiving Lawyer continue to review the electronic document or file that appears to include metadata containing Confidential Information?

The District of Columbia bar ethics committee concluded that a Receiving Lawyer must stop reviewing an electronic document or file when the Receiving Lawyer has actual knowledge that the Sending Lawyer did not intend to disclose Confidential Information in the metadata contained in an electronic document or file. DC Ethics Op. 341 (2007). The District of Columbia committee relied on its version of Rule 8.4(c), which provides that "It is professional misconduct for a lawyer to . . . engage in conduct involving dishonesty, fraud, deceit or misrepresentation." The California Supreme Court likewise concluded that a Receiving Lawyer must stop reviewing materials when it is "reasonably apparent" that there was no intent to disclose Confidential Information.[5] *Rico v. Mitsubishi Motors Corp.,* 42 Cal. 4th 807 (Cal. 2007).

The Committee disagrees with these decisions. The Committee believes that Rule 4.4(b) and (c) are the more specific rules, and that these rules trump the more general requirements of Rule 8.4(c). Therefore, where the Receiving Lawyer has no prior notice from the sender, the Receiving Lawyer's only duty upon viewing confidential metadata is to notify the Sending Lawyer. *See* RPC 4.4(b). There is no rule that prohibits the Receiving Lawyer from continuing to review the electronic document or file and its associated metadata in that circumstance. However, where the Receiving Lawyer has prior notice from the sender of the inadvertent transmission of confidential metadata, Rule 4.4(c) does prohibit the Receiving Lawyer from reviewing the electronic document or file.

As the Committee noted in Opinion 108, other considerations than the Receiving Lawyer's obligations under the Rules may come into play, including professionalism and applicable substantive and procedural law. Once the Receiving Lawyer has notified the Sending Lawyer, the lawyers may, as a matter of professionalism, discuss whether waiver of privilege or confidentiality has occurred. In some instances, the lawyers may be able to agree on how to handle the matter. *See* RPC 4.4, comment [3]. If this is not possible, then the Sending Lawyer or the Receiving Lawyer may seek a determination from a court or other tribunal as to the proper disposition of the electronic document or file, based on the substantive law of waiver.[6] *See* CBA Formal Ethics Op. 108, "Inadvertent Disclosure of Privileged or Confidential Documents" (2000).

NOTES

1. This Opinion is not intended to be a technical primer on metadata or methods to control metadata. Such a task would be beyond the expertise of the Committee, and any primer would inevitably become obsolete almost immediately.

2. The Pennsylvania Bar Association Committee on Legal Ethics declined to take a position. Instead, it summarized the rationales reached by others. It then concluded that there is no rule that would be applicable in all circumstances, and that the determination of how to address inadvertently disclosed metadata should be left to the individual Receiving Lawyer based on his or her analysis of the facts. Pennsylvania Bar Ass'n Comm. on Legal Ethics and Prof. Resp. Formal Op. 2007-500.

3. The Committee rejects the notion that a lawyer is unethical if the lawyer configures word processing software in this manner. Indeed, it may be that a lawyer should configure word processing software in this manner so that the lawyer routinely sees redlining or embedded comments in the lawyer's own documents, thus reducing the chance that the lawyer would inadvertently send such data to opposing counsel or a third party.

4. If the Receiving Lawyer receives notice before reviewing an electronic document that the electronic document contains Confidential Information in metadata, then Rule 4.4(c) applies. The Receiving Lawyer shall not review that electronic document and shall abide by the sender's instructions as to its disposition.

5. The California Supreme Court upheld the disqualification of a lawyer who continued to review materials after the lawyer had concluded that the materials contained Confidential Information that appeared to have been inadvertently produced.

6. This opinion does not address the legal issue of waiver. In some circumstances, a court may determine that the transmission of some Confidential Information waives any protections against disclosure of that Confidential Information or related Confidential Information. A Receiving Lawyer who believes that such a waiver may have occurred may ask a court to determine the issue. That is beyond the scope of this opinion.