

Ethics and Technology



Attorney Nerino Petro
Practice Management Advisor
State Bar of Wisconsin
Law Office Management Assistance Program
800.444.9404 ext 6012
practicehelp@wisbar.org



**STATE BAR
OF WISCONSIN**

Practice411TM
Law Office Management
Assistance Program

CONTENTS

Introduction	2
Applicable Model Rules	3
Your office is your castle	4
Operating System.....	5
E-Mail Security	6
Spyware/Anti-Spyware/Faux Anti-Spyware.....	7
Intrusion Detection Software (IDS)	9
Firewalls	10
Document Security.....	11
Data Protection.....	12
Metadata	13
Metadata - What Is It and What Are My Ethical Duties?	13
The Ethics of Metadata 2008	18
Examples of what can be found in Microsoft Word Documents:	19
Sharing a Computer Network	20
Backup.....	21
Cell Phone Security	22
Wireless LANs	24
Mobile Security	25
Discarding Old Equipment	27
Electronic Discovery.....	28
Legal Research	29
The Cost of Free	30
Don't be an idiot: Backup your data	31

Acknowledgments:

I have had the honor and privilege to work and share information and the stage with a number of very knowledgeable and wonderful people. I'd like to thank Attorney Terrence Dunst - Bakke Norman SC, Catherine Sanders Reach -ABA Legal Technology Resource Center, Laura Calloway Director - Alabama State Bar Practice Management Assistance Program, and Reid Trautz - Director of the AILA Practice and Professionalism Center for their contributions to portions of these materials.

INTRODUCTION

As computer technology becomes more entrenched within the legal profession, lawyers must be aware of the potential pitfalls that can arise based on our ethical obligations. Because of these additional self-imposed professional obligations, we cannot merely rely on the standard of care applicable to other businesspersons. Lawyers must take special efforts to make sure our use of technology comports with our profession's ethical standards. Furthermore, as the use of technology becomes more commonplace, attorneys may be required to expend greater effort to comply with our ethical rules. What passed for confidentiality five years ago, may not meet the required standard today.

The Rules of Professional Conduct require a minimum standard; however, lawyers must also competently use technology or face the wrath of their clients via a malpractice action. Such suits often are related to a breach of one or more ethics rules.

Understanding the ethics issues is the first part of the on-going battle to protect data. Understanding the safety issues that face lawyers and law firms is also necessary. Once identified within a law firm, solutions can be implemented to protect the data, the firm's clients, and the lawyers. Many of those solutions are suggested below; however, these solutions are primarily for solo and small firm practitioners, not larger firms.

There are several rules of professional conduct, which combine to require that lawyers exercise great care in protecting their electronic information.

Although technology may impact with most or possibly all of the Rules, the following Rules will be the focus of this presentation.

Rule 1.1 Competence
Rule 1.3 Diligence
Rule 1.6 Confidentiality of Information
Rule 5.1 Responsibilities of a Partner or Supervisory Lawyer
Rule 5.2 Responsibilities of a Subordinate Lawyer
Rule 5.3 Responsibilities Regarding Nonlawyer Assistant
Rule 7.1 Communication/Advertising Applicable Standards

ABA Model Rule 1.6 addresses confidentiality of information. Sub-part (a) of this rule prohibits a lawyer from revealing information relating to a client's representation unless the client approves the release of information, the disclosure is necessary for the representation and impliedly authorized, or the lawyer is otherwise authorized or required by the rule to reveal the information. This rule covers not only information directly relating to the representation, but any information which might lead to the discovery of confidential information.

ABA Model Rule 1.9(c) extends the requirement against disclosure of confidential information to the confidential information of former clients, and ABA Model Rule 1.18(b) creates a similar obligation in favor of potential clients.

Lawyers who have supervisory responsibility for other lawyers and law firm staff are further constrained by ABA Model Rules 5.1 and 5.3, which require them make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the supervised lawyers and staffers conform to the Rules of Professional Conduct, including the rules regarding confidentiality of information.

Although ABA Model Rule 1.15 on safekeeping of client property and its comments do not specifically refer to electronic information belonging to a client, a reading of the rule makes it clear that future ethical decisions might reasonably be expected to extend its reach to such property. Most jurisdictions require that records of client property be kept for a minimum of five years. In an age in which a client's documents are most useful in their electronic state, it is no stretch of the imagination to expect that a lawyer's duty to protect those documents might extend to protecting them in their native format.

So if all these rules require lawyers to protect their electronic information, what steps must lawyers take and what standards must they meet? While there is a dearth of reported opinions and cases in this area, the comments to the rules give us some guidance.

Comment 15 to ABA Model Rule 1.6 requires that a lawyer act competently to safeguard information against inadvertent or unauthorized disclosure of confidential information. Comment 16 to the same rule requires that when transmitting information, a lawyer must take reasonable precautions to prevent the information from coming into the wrong hands. The lawyer is not required to use special security measures if the method of communication affords a reasonable expectation of privacy, but the comment goes on to say that special circumstances may warrant special precautions. In determining whether a lawyer's actions were reasonable, one should look to the expectation of confidentiality, the sensitivity of the communication and the extent to which the privacy of the communication is protected by law or confidentiality agreement. The comment leaves the final authority regarding reasonableness in the hands of the client. By stating that a client may require a lawyer to implement special measures, or may consent to use of a means of communication would otherwise be prohibited by the rule.

Thus, it would seem that the rules do not require complete success, but do require that a lawyer, especially one whose electronic information has been compromised, to demonstrate that reasonable steps were taken to protect the digital information in light of what the reasonable lawyer would know and understand about such matters.

Do you know as much as about protecting your data as this hypothetical *reasonable* lawyer?

Like a medieval castle, your office is your fortress. Multiple walls are needed to keep intruders out, and additional precautions are needed to protect the King from internal dangers. In fact, some studies show that more techno-dangers come from within a business than from the outside.

What follows is an overview: detailing all possible threats and the possible protective steps to counter them is beyond the scope of this paper. Instead, it will focus on threats we believe you are most likely to encounter and common sense solutions that you can take to protect yourself and your data from falling victim to current security threats.

Information security does not have a one product, one-size-fits-all solution: Hackers and other criminals target some high-profile firms, because of the nature of their work, while others firms go unnoticed. Some firms may have a VPN, while another does not.

Each firm must implement appropriate security solutions while remaining vigilant to new dangers. Your reputation and success rest upon this vigilance. Protecting your computer and data is truly an instance where you are better to be proactive, to “go on the offensive” to take steps to safeguard yourself, your firm and your clients. So man the walls, raise the drawbridge and prepare for battle because the enemy is at the gate intent on pillaging what you hold dear!

OPERATING SYSTEM

The first place to start in protecting yourself and your data, is by keeping your Operating System (“OS”) up to date. Microsoft Windows is the most widely used OS and is therefore the primary target for HACKERS and CRACKERS. No protection plan that you undertake will survive contact with the Cyber-Barbarians if you fail to keep your OS up to date. If you use Mac OS X or Linux, you’re not out of the cross hairs: vulnerabilities have been found in both of these and as they become more widely used, the number of attempted exploits will also increase.

Updates

Windows XP provides for several different options for automatic updates which can be activated as follows:

Click Start > Control Panel > Performance and Maintenance > System > Automatic Updates:

▶ This method will work if using the Category View for folders.

or

Click Start > Control Panel > System > Automatic Updates.

▶ This method will work if you are using Windows Classic view for folders.

Make sure that the “Keep my computer up to date” checkbox is marked.

Then select from one of the three options for downloading and installing updates.

▶ The first two options allow you to control and requires you to be involved in installation of each update. The third option will automatically download and install updates on the schedule you establish, thereby automating this process.

▶ Microsoft now publishes security updates on the Second Tuesday of every month.

You can also manually scan your system and download updates by accessing the Windows Update website at: <http://v4.windowsupdate.microsoft.com/en/default.asp>

or

Click Start > Help and Support > Keep your computer up-to-date with Windows Update.

▶ This will take you to the Windows Update website which you can allow to scan your system for updates.

▶ Critical Updates and Service Packs are those updates that affect security and vulnerabilities of your computer – these should be downloaded. Windows Updates may include helpful updates, but also updates that you may not want, so review these before downloading. Driver Updates affect device drivers for your system and you should review these and consider them carefully before downloading.

Anti-Virus Protection is essential for every computer in a law firm or lawyer's home office. The first line of defense is to have an Internet usage policy for the office or firm. Require all lawyers and staff to only open email attachments from reputable sources. Do not allow non-work related attachments to be opened.

Just having the software is not enough. You must download the latest antivirus definitions to ensure the software contains the most up-to-date detection and prevention. Commercial anti-virus software publishers often sell update subscriptions for about \$30 per computer per year; enterprise licenses are much cheaper per seat.

Encryption is not required under the confidentiality rules in Wisconsin or Illinois and a number of others leave it up to the lawyer to decide. However, a growing number of states are enacting data protection laws which may require encrypting emails and other digital data. These laws and their requirements are discussed in the Data Protection section of later in this paper. If the information you intend to put in the email is so sensitive that you would not send it by un-bonded courier or regular mail, then it probably needs to be encrypted. Also discuss the matter with your client; if they want it encrypted, then do it. There are commercial encryption products available, including on-line services. Work with your client to find the best solution for sending and receiving encrypted email.

Misaddressed emails can also breach attorney-client confidentiality. Like a fax sent to a wrong phone number, an errant email can do as much damage. In Microsoft's Outlook consider turning off the address "AutoComplete" function to avoid mistakes; remind staff to always double-check the addressee in each outgoing email. Finally, while I know of no authority that disclaimers in the email work, it still seems like a good idea. Try adding it above the message, rather than at the end, this will serve as a warning to any unintended reader.

Clearly, spam filters become more important each day. Spam filters prevent our Inboxes from overloading, but spam filters are not fool-proof. Some spam gets through, while some important messages do not. Be sure to open your "Suspected Spam" folder on a daily basis to make sure nothing important was filtered out by mistake.

Retaining client emails is becoming more of an issue. Is an email message more like a letter or a phone call? If it is a letter, doesn't it belong in the client's file? If not, shouldn't it be discarded? Check your state's legal ethics opinions for more guidance in this area.

There are many products that will remove adware and spyware from your computer; however, your first line of defense is your web browser. Which browser you use can have a lot to do with how much time you spend clearing your computer of malware on a regular basis.

Anyone who is even vaguely knowledgeable about the Internet knows that Microsoft Windows and Internet Explorer are both full of security holes and are very subject to viruses and malicious attacks. Even if you have hardware and software firewalls between your computer and the Internet and keep your virus software scrupulously up to date you are subject to the plague of pop-up and pop-under ads, and the ghoulies they may contain, which some web sites – even reputable ones, throw at you.

To make Internet Explorer safer to use, consider disabling the ActiveX controls. This can easily be done, but it does reduce the functionality of IE. Some IE users object to this, but many find no appreciable difference in their web browsing experience. It may be better to be safe than sorry.

Dan Pinnington, in his guide *Managing the Security and Privacy of Electronic Data in the Law Office*, suggests the following settings: For Internet Explorer versions 5.0 and later, click on Tools, then select Internet Options. Next, select the Security tab. Click on the Internet icon (the globe), and then click on the Default Level button to remove any custom settings. Next, click the Custom Level button. This will open the Securities Settings dialog box. In the ActiveX Controls Plug-Ins section of that box (at the top), configure the following settings as noted:

Download Signed ActiveX Controls: Prompt
Download Unsigned ActiveX Controls: Disable
Initialize and Script ActiveX Controls Not Marked as Safe: Disable
Run ActiveX Controls and Plug-Ins: Prompt
Run ActiveX Controls Marked Safe for Scripting: Prompt

To save your changes, click OK, answer Yes to the Are you sure you want to change the settings for this zone questions, then click Apply, and OK.

Another alternative is not to use Internet Explorer, but a more secure competitor: The Firefox browser.

Firefox is the free browser from Mozilla, the non-profit web development offshoot of Netscape. They have worked to produce a new browser to compete with Internet Explorer, and to clear up some of the problems Microsoft either can't, or won't fix. It's a winner, as evidenced by the fact that it's already captured 15% of the worldwide browser market. That may not sound like much, but a good deal of that steady growth has been in the last couyear.

The browser has a nice, clean, simple look, which is very easy to modify. It comes set up with the requisite buttons for forward and back, stop, reload and home, and it's easy to go into the preferences and drag dividers, printer buttons, a little clock to show your browsing history, and other useful buttons onto the toolbar. For those who are used to using a Google toolbar on their browser, it even comes with a little window you can use to do a Google search without even having to call up Google.

Getting the browser is easy. Just go to <http://www.mozilla.com/>, download it, and double click on the downloaded file to install. It will even ask you if you'd like to import your bookmarks from Internet Explorer!

Once you have a more secure browser, it's time to look at some anti-spyware products to sweep and clean up your computer. The chances are very good that, even if you haven't experienced the slowdowns and crashes that are the alarm-bell that malware is present, you have some of it on your computer.

The job of a good anti-spyware program is twofold: first it should locate and remove malware already resident on your computer; then, it should block new programs from downloading themselves in real time. Fortunately, you have many products from which to choose, and some of them are pretty good.

According to product reviews in issues of PC Magazine and PC World, some of the most effective malware detector/removers are Spyware Doctor from PC Tools (www.pctools.com) and Spy Sweeper from Webroot Software, Inc. – www.webroot.com. At around \$30 for a one-year subscription, for individual users, you can't afford not to have one of these programs on your computer.

Counterspy from Sunbelt Software is also getting stellar reviews from the computer press, and at \$20 is a real bargain.

Ad-Aware from Lavasoft (www.lavasoftusa.com) is another well-known and fairly effective program, which comes in both free and fee-based versions.

The free version is Ad-aware Personal. It's designed to provide protection from data-minders, aggressive advertising, and selected other malware including some dialers and browser hijackers. Ad-aware Personal does not include real-time blocking, but is a great tool in conjunction with other free or paid programs to keep you home computer free of spyware.

There are also two paid versions of the software: Ad-aware SE Plus and Ad-aware Professional. Ad-aware SE Plus includes all the features of the personal edition along with enhanced features such as real-time monitoring that allow you to delete malware before it infects your system. Ad-aware SE Plus for business or home use runs about \$40. The Professional edition contains additional features which allow you to analyze running processes, and costs about \$50. The Lavasoft site also offers a shareware registry editor called Reghance™.

While these spyware removal tools are great, the next generation of protection prevents the malware and spyware from loading onto your computer at all. These products for your web browser act like anti-virus software for e-mail. SpywareGuard and SpywareBlaster are two such products. These freeware products from Javacool Software help keep the bad stuff out, but as with many of these new programs, there may be compatibility issues.

For additional information about spyware prevention software, click over to www.2-spyware.com. This site contains comparisons of anti-spyware products as well as instructions for dealing with spyware.

The bottom line: None of the currently existing anti-spyware programs will stop or remove everything that the evil goblins lurking on the Internet can throw at your computer. Existing programs are constantly being updated, and new programs to combat new threats are constantly being developed. A combination of two or more programs, free and fee, is needed to give your computer the greatest possible protections.

INTRUSION DETECTION SOFTWARE (IDS)

Intrusion detection software fills the gaps between firewalls, anti-spyware, and anti-virus software. Hackers, spyware purveyors, and on-line criminals know where these gaps in protection exist, and are working hard to exploit them. IDS stops trojans, worms, hijackers, and other malicious programs from getting in to your computer, but also prevents them from executing once inside your firewall. Again, no solution is perfect, but this new type of security software is important to own.

Prevx Pro (www.prevx.com/) is one such product from Prevx Ltd. Another is WinPatrol (www.winpatrol.com/), which also receives high marks in the software press. Symantec's (www.symantec.com/) small business solutions also promise intrusion prevention and Untangle's (www.untangle.com) open source Network Gateway also provides intrusion prevention.

According to the Wikipedia, a firewall is a piece of *hardware or software* that functions in a networked environment to prevent some communications forbidden by the security policy, analogous to the function of firewalls in building construction. It has the basic task of controlling traffic between different zones of trust. Typical zones of trust include the Internet (a zone with no trust) and an internal network (a zone with high trust). The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.

Typically, small businesses have used software solutions to control unwanted access to network and internet connected computers. These solutions include a basic firewall in Windows XP and a slightly better version in Windows 7, Zone Alarm (www.zonealarm.com), Comodo (www.comodo.com), Kerio (www.kerio.com) and various versions from Symantec, McAfee, Trend Micro, Grisoft and others.

Larger enterprises often use firewall appliances from companies such as SonicWall (www.sonciwall.com), Barracuda Networks (www.barracudanetworks.com), WatchGuard (www.watchguard.com) and Untangle (www.untangle.com) —integrated hardware solutions to stop unwanted hackers and others. However, some of these appliances are now being targeted at smaller businesses; small to medium size law firms should consider this as a possible alternative to software alone.

There are also a number of free or open source products, including Untangle Lite Package which is free (www.untangle.com) and provides a firewall as well as anti-virus, anti-intrusion detection, site filtering and more. Untangle also offers a paid version which can be installed on a computer that you own or you can buy it on a computer directly from Untangle. This version which includes live technical support and advanced management features starting at \$40.00 per month for 1 to 10 users. Both Comodo (www.comodo.com) and Kerio (www.kerio.com) offer software firewalls.

Documents are the lifeblood of attorneys. They contain the work product of the firm. Many lawyers share electronic documents with clients, co-counsel, opposing counsel and the courts via email, efilings, and extranets. These documents more often than not contain sensitive client information. Lawyers have a duty to preserve the confidentiality of that information. Electronic documents, unprotected, can be copied, printed, edited, and reused by others.

One step law firms can take to protect sensitive information is to use password security on electronic documents. Microsoft and Corel office suites offer the ability to password protect documents. In MS Word 2003 under "Tools" "Protect Documents" you can limit editing to read-only, comments, and track changes. Under "Tools" "Options" "Security" you can enable password protection to open or modify a document. There are also privacy options, such as "make hidden markup visible when opening or saving" and "warn before printing, saving, or sending a file that contains tracked changes or comments". You may consider some of the security options within the firm when they make sense to protect client information or the integrity of the document.

Another way to protect documents from unwanted changes or exposure is to consider publishing to PDF. Using Adobe Acrobat or other PDF writing program, you can convert word processing files to PDF before sharing them. In Adobe Acrobat users can "lock down" documents, disallowing printing, copying, editing, commenting or even opening the document. You can encrypt the file or use secure digital signatures and authentication protocols. Attorneys can make sure that the document is used in the way they want, without exposing it to alteration or copying.

A growing number of states are passing data protection laws that govern what digital information must be protected and how it is to be protected. California passed the first such law in 2003 and has been followed by Massachusetts number of other states. These laws generally require firms to prevent the unauthorized disclosure of personal information which is generally interpreted to mean any information that can be linked to an individual such as a person's name in conjunction with other information such as a social security number, driver's license number, credit card number or bank account number where wither piece of information is not encrypted. If a "breach" occurs which results in an actual acquisition of personal information by a third party or the firm reasonably believes that such a disclosure has occurred, the firm must notify the person or persons whose information has been disclosed without unnecessary delay.

Many of these laws also require that portable devices that contain personal information be encrypted which means that notebook computers, smart phones, DVDs, portable data storage devices, etc. all be encrypted to protect the information they contain. Many of these laws also contain requirements that if a firm is sending personal information electronically outside of a secure network (think the Internet rather than a firm computer network) it must be encrypted. So if the email you are going to send from or into one of these states contains any combination of information that triggers the statute, the email will need to be encrypted. However, while some of these laws, Nevada and Massachusetts spell out much of what is required and the standards, they are in general terms leaving many questions unanswered.

There are a number of steps that firms can take to protect themselves.

1. Secure access to your network and computers. Everyone in your office should have their own user name and password to access computers and network resources.
2. Install network gateway security devices to prevent intrusions and to serve as bi-directional firewalls checking both incoming and outgoing electronic communications.
3. Do not give everyone in the office access to everything on the network unless they absolutely must have access to it. Limit full access to specialized systems such as accounting and payroll to only those that work with it. Not every user needs to be an administrator and assign network rights accordingly. A general typist doesn't need rights to install software or makes changes to security settings.
4. Use encryption on your data files. These can operate seamlessly and provide that unless someone has the proper password the files remain unreadable by any method. Microsoft has its [BitLocker](#) technology with certain versions of Windows and MS Server software. A free and open source alternative that is extremely popular (I use it myself) and works on a variety of operating systems is [Truecrypt](#). Truecrypt allows you to create encrypted files, folders or entire drives and has a large development and support community. There are a number of other products available including [SecureDoc](#), [PGP Whole Disk Encryption](#) and [MEO](#) encryption software.
5. Use encryption on your email when necessary. While there are a number of ways to encrypt email, the option that is most widely recognized for this is known as Public Key Infrastructure (PKI). This process uses two keys which are unique to you or your firm. Using mathematical formulas which link the two keys, a firm publishes its public key while it keeps its private key secret. When you want to send encrypted email to someone, you obtain their public key to encrypt it and the recipient then uses their private key to decrypted. The strength of this systems is that the public key cannot be used to discover the private key. There are also encryption methods that use only one key which means that it must be transmitted to the recipient to open the file (this is similar to using a password to lock a file and then having to provide the password to the recipient). Products include [PGP Desktop Email](#) , [TrustTone Encryption for MS Outlook](#), [Postini Email Encryption](#) and [Mirramail Secure Email](#). Another option is to obtain a digital certificate to take advantage of the built-in digital signature and encryption features found in some email software. You can obtain a free secure email certificate from [Comodo](#) or purchase one from Verisign or another company.

Metadata is the information hidden behind your words; it includes the name of the author, the date created and last edited, as well as the undo/redo history. Metadata resides in almost every type of electronic document or file created in a law office—especially files created using the Microsoft Office suite. Therefore, when you send the settlement proposal as a Word document, the receiving party may be able to see your edited changes or whether the document is original to that client or a form created for someone else. Clients and others may be able to easily view some of the data to see if any changes you made—say to the final top-dollar offer contained in your letter created in MS Word. The disclosure of the metadata could be a breach of confidentiality, not to mention highly embarrassing. The ABA recently issued ABA Formal Opinion 06-442 on Review and Use of Metadata and the Maryland State Bar issued MD Ethics Docket No. 2007-09. These opinions generally state that it is the sending attorney's responsibility to remove metadata they do not wish to expose to the recipient. These opinions differ from the New York State Bar, Florida Bar, Alabama Bar and DC Bar opinions on metadata, which also warn attorneys to be aware of what they are sending out via metadata, but also warn recipients that it is unethical to review or mine documents for metadata. To avoid problems with metadata, consider converting a document or file to PDF format to eliminate much of the metadata, or try a metadata removal tool, such as the Metadata Assistant from www.payneconsulting.com or iScrub (<http://esqinc.com/section/products/2/iscrib.html>).

METADATA - WHAT IS IT AND WHAT ARE MY ETHICAL DUTIES?

By Jim Calloway

An attorney looks in his inbox and finds a long-awaited settlement proposal from opposing counsel attached to an e-mail. The attorney opens the document and hits the print command. While the document is printing, the attorney eagerly looks at the monitor for details. "Good, the settlement figure is probably still too high, but very close to reasonable." The document is quite short, actually. How long could drafting it have taken? Idly, the attorney clicks on the properties tab and sees the document was open on opposing counsel's computer for three hours.

"Wait," the attorney thinks. "Didn't I get that metadata scrubber utility? They said it could be used to look at metadata, too. He locates the icon and clicks on it. In a few moments, he is reviewing the revision history of the document. It looks like several documents were combined and then a lot of deletions were made at the end. The lawyer pulls up a large block of deleted text and begins to read, "Notes. Client is desperate to recover something and not face the PR disaster of receiving nothing at trial. Offer \$100K. But get it settled before end of month even if we have to take half that."

The lawyer sits up with a cold chill, quickly closing the document. Then he stands up and starts pacing the room. What had the lawyer done? What was the lawyer supposed to do going forward? Was there something wrong with taking advantage of this information? Why does he already feel guilty? Finally, with a flash of anger, he thinks, "Why was that opposing lawyer dumb enough to send me that information?"

As the above example should illustrate, every lawyer needs to understand a few basic things about metadata. The legal ethics implications of metadata "mining" are no longer just of interest to the lawyers processing electronic discovery or the ethics mavens. There is little dispute at this point over the pervasiveness of metadata that can be contained in digital documents and other computer-generated files. It is important to understand that for computer files, that "deleted" often does not really mean gone. This has been obvious for some time to those of us who have learned the magic of the Ctrl + Z (Undelete) keystroke combination. I smile almost every time I use it.

In many law firms, proposed documents are circulated among lawyers by e-mail with each adding their own comments or suggestions. These comments from other lawyers in the firm attached to the document are ultimately deleted and never meant to be communicated outside of the office. But these comments might be revealed by anyone with a copy of the document. Document revisions may be revealed by using the right tools.

The ethical implications of one lawyer examining the metadata in a file received from another lawyer have generated a lot of discussion. This article will cover the legal ethics opinions issued so far and give you tips on how to avoid exposing confidential information unintentionally via metadata.

Let us note that these concerns are not present when examining the metadata contained in digital documents produced as a part of the discovery process. It is now considered routine to examine important documents that are a part of the evidence if there is an issue that might be explained with metadata. Metadata scrubbing of the electronic files received from a client related to litigation might be viewed very critically by the courts.

Just exactly what is metadata?

Simply put, metadata is data about data. For our purposes, we will refer to metadata as any data that is contained in a digital file (such as an e-mail, spreadsheet or word processing document) that is not readily apparent when normally viewing the file. For example, none of us are surprised that when we view a document, we can click on the “Properties” tab for more information, like the number of words in the document or the date it was last edited. But there are other types of metadata that can be viewed with special tools.

For more detailed explanatory information on metadata, see the Wikipedia entry at <http://en.wikipedia.org/wiki/Metadata>. Here is a more official (and non-wiki-editable) example of the lawyer’s concerns:

“Metadata may reveal who worked on a document, the name of the organization that created or worked on it, information about prior versions of the document, recent revisions, and comments inserted in the document during drafting or editing, the committee said. The hidden text may reflect editorial comments, strategy considerations, legal issues raised by the client or the lawyer, or legal advice provided by the lawyer.” ABA/BNA Lawyers’ Manual on Professional Conduct 21 Current Rep. 39 (2004)

There is nothing nefarious about metadata. But, there has been a great deal of discussion about acceptable uses of metadata in the legal ethics community.

One of the early opinions about metadata was issued after a highly publicized situation where a Florida law firm examined a pleading that was electronically mailed to them and located, according to press accounts, deleted comments between attorneys and some comments that had been given to the attorneys by the client. The lawyer who directed that the document be e-mailed was unaware of metadata issues and was said to have been persuaded by a lawyer in the other firm to e-mail the pleading instead of faxing the document. Depending on your point of view, this may appear to be either a sneaky and underhanded trick by one lawyer or a lapse in judgment by the transmitting lawyer because many were aware of metadata. (The issue has been widely known and discussed since 1998.)

But, before we get to Florida’s response to this issue, let’s cover existing ethics opinions on this topic in chronological order. The issue as it is framed today is 1) if one receives a document from opposing counsel, is it appropriate to examine the document’s metadata? and 2) if one becomes aware a document so received contains revealing metadata, what should be done in response? Is one required to either disregard it or reveal the discovery to opposing counsel immediately?

The first legal ethics opinion about metadata came out in December 2001. New York State Bar Opinion 749 stated, “A lawyer may not make use of computer software applications to surreptitiously ‘get behind’ visible documents or to trace e-mail.” It is probably instructive to recall that at about this time ethics opinions were being promulgated saying that lawyers should not use unencrypted e-mail for client communication either. Those opinions were later withdrawn or revised.

Approximately three years later, the New York State Bar came out with Opinion 782. In this opinion it was acknowledged that when sending documents by e-mail, “a lawyer must exercise reasonable care to ensure that he or she does not inadvertently disclose his or her client’s confidential information.” The opinion restated the rule of Opinion 749 as “an obligation not to exploit an inadvertent or unauthorized transmission of client confidences or secrets.”

This would not be the last opinion to consider metadata transmission as unintended, inadvertent or unauthorized; even though the sender clearly intended to transmit the document, although perhaps without full understanding of the implications or existence of metadata.

In December 2005, the Florida Bar Board of Governors asked for an ethics opinion on the mining of metadata from electronic documents. The Florida Board of Governors made national headlines in the legal press when this matter first came to their attention as several members were quoted as saying they had never heard of metadata. At the same meeting where the board asked for an ethics opinion, the board also voted unanimously for a motion to express its sentiment that metadata mining is something lawyers should not do. *Florida Bar News*, Jan. 1, 2006.

In August 2006, the American Bar Association weighed in with Formal Opinion 06-442. This was viewed by many as a rejection of both the New York approach and the anticipated opinion from Florida. Formal Opinion 06-442 stated:

“The Model Rules of Professional Conduct do not contain any specific prohibition against a lawyer’s reviewing and using embedded information in electronic documents, whether received from opposing counsel, an adverse party, or an agent of an adverse party. A lawyer who is concerned about the possibility of sending, producing, or providing to opposing counsel a document that contains or

might contain metadata, or who wishes to take some action to reduce or remove the potentially harmful consequences of its dissemination, may be able to limit the likelihood of its transmission by 'scrubbing' metadata from documents or by sending a different version of the document without the embedded information."

In September 2006, Florida Ethics Opinion 06-2 was released after much anticipation. The ethics group stated "[a] lawyer who is sending an electronic document should take care to ensure the confidentiality of all information contained in the document, including metadata." But they also determined, in accordance with the opinion of the Florida Bar Board of Governors, that a recipient lawyer should not examine a document for metadata.

The Alabama Bar issued Ethics Opinion Number: 2007-02 on March 14, 2007. This rather informally written opinion adopted the New York Bar position. "[T]he Commission believes that an attorney has an ethical duty to exercise reasonable care when transmitting electronic documents to ensure that he or she does not disclose his or her client's secrets and confidences.... Just as a sending lawyer has an ethical obligation to reasonably protect the confidences of a client, the receiving lawyer also has an ethical obligation to refrain from mining an electronic document....The unauthorized mining of metadata by an attorney to uncover confidential information would be a violation of the Alabama Rules of Professional Conduct." The commission does note a "possible" exception in the case of documents received via electronic discovery. This opinion rests on some questionable assumptions. The assumption is made that the only reason one might look at metadata would be to discover confidential client communication and attorney work product. But, in fact there are many other reasons to examine metadata, including discovering the date of creation or transmission of documents.

The District of Columbia Bar in Opinion 341 adopted a "look before you leap" approach. This opinion states: "A receiving lawyer is prohibited from reviewing metadata sent by an adversary only where he has actual knowledge that the metadata was inadvertently sent. In such instances, the receiving lawyer should not review the metadata before consulting with the sending lawyer to determine whether the metadata includes work product of the sending lawyer or confidences or secrets of the sending lawyer's client."

Actual knowledge seems to incorporate a very high standard. One has to consider whether many lawyers would view this opinion as a "green light" to generally review metadata in almost all circumstances.

Next to issue an opinion was the Maryland Bar, with Ethics Docket No. 2007-09, which stated: "[s]ubject to any legal standards or requirements (case law, statutes, rules of procedure, administrative rules, etc.), this Committee believes that there is no ethical violation if the recipient attorney (or those working under the attorney's direction) reviews or makes use of the metadata without first ascertaining whether the sender intended to include such metadata."

This opinion was heavily influenced by the fact that Model Rule of Professional Conduct Rule 4.4(b), which states that "[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," was never adopted in Maryland.

Pennsylvania soon followed with Pennsylvania Opinion 2007-500, which could be termed indecisive. After reviewing the existing opinions, the committee concluded that "it would be difficult to establish a rule applicable in all circumstances and that consequently the final determination of how to address the inadvertent disclosure of metadata should be left to the individual attorney and his or her analysis of the applicable facts."

And, in November 2007, Arizona joined those jurisdictions that endorsed the idea that, while it was the responsibility of the transmitting lawyer not to send out some types of metadata, it was also the responsibility of the lawyer who receives it not to look at it. The opinion states:

"Under Arizona's version of ER 4.4(b), a "lawyer who receives a document and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender and preserve the status quo for a reasonable period of time in order to permit the sender to take protective measures." While it might be argued that ER 4.4(b) is inapplicable because the document was not inadvertently sent, only the metadata embedded therein, we think that is an insubstantial distinction. If the document as sent contains metadata that reveals confidential or privileged information, it was not sent in the form in which it was intended to be sent, and the harm intended to be remedied by ER 4.4(b) is the same."

Earlier this year the Colorado Bar issued Ethics Opinion number 119 (May 17, 2008.) In it, the Colorado committee concluded that the primary responsibility is on the transmitting lawyer not to send out metadata. It stated: "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.”

....

“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.”

Colorado, with the benefit of improved understanding of the nature of metadata and the prior opinions to review, seems to have a quite logical and practical position. First, it is the responsibility of the transmitting attorney not to send out metadata containing confidential information. Secondly, there is no justification for an artificial rule prohibiting lawyers from looking at metadata as the vast majority of it is benign and involves no confidential information. Third, if a review of metadata reveals what appears to be confidential information, the receiving attorney should assume that it was sent unintentionally and notify the opposing counsel. Then the attorneys may be able to enter an agreement as to how to handle the information. Failing that, then the courts may be called upon to determine if any confidentiality has been waived or if some other appropriate order is required.

Conclusion

There’s no doubt that examining the metadata behind opposing counsel’s e-mail or transmitted documents seems unseemly and inappropriate to many. But the existence of metadata is a fact. It is a fact we will have to deal with, just as we have to deal with the fact that people make mistakes.

In this writer’s view, the problem with the opinions seeking to restrict viewing of metadata is that they attempt to impose a standard uniquely on the legal profession. Nothing restricts viewing of metadata in documents by private investigators, law enforcement officers, computer forensic examination professionals and every other individual without a law license, even the lawyer’s clients. What if the lawyer’s client in the first example had requested the document be forwarded to the client, examined the document’s metadata and then sent instructions to counteroffer at 50 percent without even telling the lawyer what happened?

Even if a consensus developed that lawyers should not look at metadata, can one assume the risk that the lawyer on the opposing side, or someone else, will not look?

In this writer’s view, the key is to avoid sending out documents with metadata that could disclose confidential information. Comparing metadata to a wrongly sent fax or e-mail is questionable and the idea that lawyers will be prohibited from examining metadata while parties, law enforcement officers and private detectives will be free to do so seems artificial at best. The Colorado rule that one must disclose receiving confidential information via metadata before acting on it seems to strike a rational balance. The best rule is for law firms to develop best practices internally to keep metadata from “escaping” in the first place. Using PDF format for e-mail attachments generally instead of Word, WordPerfect, Excel or PowerPoint will go a long way toward alleviating the problem.

It is often the case to conclude legal analysis of an emerging issue with a note that we will have to watch for future opinions and developments for more instruction. Here, we take a contrary view. It would be better for lawyers, clients and the judiciary if this issue simply “went away” as all law firms strive to never transmit electronic files that might unintentionally disclose confidential information.

Author’s note: the opinions contained herein are those of the author only and not the Oklahoma Bar Association. In fact, they may not be the opinion of the author next week. After this article went to press, the Maine Board of Overseers of the Bar released Maine Ethics Opinion #196 (10/21/2008) dealing with metadata. It is available online at <http://tinyurl.com/2cmetu7>.

Ethics Opinions on Metadata

[NYSBA Opinion 749](http://tinyurl.com/3lvzta) (<http://tinyurl.com/3lvzta>)

[NYSBA Opinion 782](http://tinyurl.com/27uc96z) (<http://tinyurl.com/27uc96z>)

ABA Formal Opinion 06-442 No longer available without payment of \$7.50 fee or annual subscription here:

www.abanet.org/cpr/pubs/ethicopinions.html

[Florida Opinion 06-2](http://tinyurl.com/sefk3) (<http://tinyurl.com/sefk3>)

[Alabama Formal Opinion 2007-02](http://tinyurl.com/24gyxys) (<http://tinyurl.com/24gyxys>)

[District of Columbia Opinion 341](http://tinyurl.com/3yhf8z) (<http://tinyurl.com/3yhf8z>)

Maryland Bar Ethics Docket No. 2007-09 is available to members only

[Arizona Bar Opinion 07-03](http://tinyurl.com/2dveuj7) (<http://tinyurl.com/2dveuj7>)

Pennsylvania Bar Association Opinion 2007-500 is available to members only

[Colorado Bar Ethics Opinion 119 Disclosure, Review, and Use of Metadata](http://tinyurl.com/5wscmj) (May 17, 2008) (<http://tinyurl.com/5wscmj>)

Guarding Against Metadata Disasters

There are many possible solutions to the issue of disclosing metadata. Some combination of the following may work best for your office. Obviously purchasing a metadata scrubber utility and using it is the best option.

Assess the situation. If this is a new document you have created this week and only you have worked on it, there may be no potentially problematic metadata contained in it.

Fax or snail mail rather than e-mail.

Copy all text (Ctrl +A, Then Ctrl + C) and Paste it (Ctrl + V) into a blank document. Note: This will carry some metadata, but not Track Changes or Deleted Comments.

Copy all text (Ctrl +A, Then Ctrl + C) and Paste Special - Unformatted Text into a blank document. Note: You lose the metadata, but all of the document formatting as well. This works great for pasting text into an e-mail, but not so well for heavily formatted legal document.)

Every time you send an e-mail attachment that you have created or edited, send it out in PDF format (with rare exceptions) Note: PDF files will contain some metadata, but that limited amount is unlikely to cause trouble. This is not practical when you are co-authoring a document with another. With co-counsel, you just need to discuss the issue. With opposing counsel, you need to use a metadata scrubber.

Microsoft Word 2002 — Review white paper at <http://tinyurl.com/5gtpv6> but consider upgrading or buying a metadata scrubber. Microsoft Word 2003 (and other MS Office products) – Download and install The Remove Hidden Data tool for Office 2003 and Office XP <http://tinyurl.com/567r6t>.

Microsoft Word 2007, Excel 2007 and PowerPoint 2007 – Remove hidden data tools are built in. No separate download required. See Microsoft instructions for Document Inspector feature online at <http://tinyurl.com/29ql2o> (Note: Computer forensics experts tell us the results from the free Microsoft tools listed above are imperfect.)

Corel WordPerfect – Upgrade to Versions X3 or X4 which have the “publish without metadata” feature. WP versions 9 and higher have the “publish to PDF” option built it as well. (WP has less potentially dangerous metadata than MS Word.)

Purchase a third-party metadata scrubber and use it. There are many such products, but we direct the smaller firm’s attention to the Metadata Assistant from www.payneconsulting.com. At a purchase price of \$79 per license, this product will also allow you to view the metadata in other files. (Direct link to retail version — <http://tinyurl.com/e2zef>. Enterprise version for more than 20 workstations available as well.) Workshare: Workshare Protect is another product for \$30.00 www.workshare.com .

About The Author

Jim Calloway is the director of the OBA Management Assistance Program and manages the OBA Solo & Small Firm Conference. He served as the chair of the 2005 ABA TECHSHOW board. His Law Practice Tips blog and Digital Edge podcast cover technology and management issues. He speaks frequently on law office management, legal technology, ethics and business operations.

Metadata - What Is It and What Are My Ethical Duties?

Published 79 OBJ 2529 (Nov. 8, 2008)

THE ETHICS OF METADATA 2008

By Jim Calloway

Metadata still remains a huge and often misunderstood topic. Since my article *Metadata - What Is It and What Are My Ethical Duties?* was published in the Oklahoma Bar Journal on November 8, 2008, I've already had several people contact me and say "Wow, I didn't know anything at all about that. Thanks." When you write something for publication, you want everyone to read it. But this is something that I believe everyone needs to read and understand, whether you agree with my point of view or not. The legal ethics piece may be particular to lawyers, but everyone needs to know about metadata. Now that the article is online, take a moment to e-mail [this link](http://www.okbar.org/obj/articles08/110808calloway1.htm) (<http://www.okbar.org/obj/articles08/110808calloway1.htm>) to lawyers you think might not be aware of the legal ethics issues relating to metadata.

Update: Of course, as soon as my article went to press covering *every single legal ethics opinion about metadata*, a new one had to emerge. You may want to read the article first before reading the following paragraphs.

On October 21, 2008, the Maine Board of Overseers of the Bar released [Maine Ethics Opinion #196](http://tinyurl.com/2fdq34l) (<http://tinyurl.com/2fdq34l>).

This opinion arrives at two conclusions:

Without authorization from a court, it is ethically impermissible for an attorney to seek to uncover metadata, embedded in an electronic document received from counsel for another party, in an effort to detect confidential information that should be reasonably known not to have been intentionally communicated.

A sending attorney has an ethical duty to use reasonable care when transmitting an electronic document to prevent the disclosure of metadata containing confidential information.

Point 2 is now largely a consensus opinion of the jurisdictions that have opined on the issue. It is certainly "good law" and good practice. Point 1 adopts the theory of several jurisdictions that lawyers are prohibited by our ethics rules from looking at certain types of data that everyone else can freely view. At least the authors insert an intent element so that it is clear some examining of metadata is OK, like looking at the formulas in a spreadsheet to make sure they are accurate. I do not disagree with the lofty sentiments and high goals, but question the practicality of this view.

Authors of the more recent ethics opinions have the benefit of being able to review the prior work that well frames the issues. As I noted in my article, Colorado in Formal Opinion 119 adopts the view that there is nothing wrong with looking at metadata. But if you stumble across confidential information, you must immediately notify opposing counsel so that you can agree how to handle it or either of you can go to court for guidance or relief. I note this because the Maine opinion specifically criticizes this approach as "a complex and perhaps impractical set of requirements for the parties," while hinting that one would have to be a computer genius to fully understand metadata anyway.

Opinions still differ about legal ethics and metadata. Links to all of the ethics opinions that are publicly available online appear at the end of my article.

November 18, 2008 in [Risk Management, Technology Trends](#) | [Permalink](#)

TrackBack

TrackBack URL for this entry:

<http://www.typepad.com/t/trackback/241185/35900030>

EXAMPLES OF WHAT CAN BE FOUND IN MICROSOFT WORD DOCUMENTS:

- Author name/ initials
- Company/organization name
- Subject, file type, location
- Date created/modified/last accessed
- Number of revisions/versions
- Previous document authors
- Total editing time
- Template information
- Hidden text (formatting)
- Comments
- OLE objects
- Macros
- Hyperlinks
- Redlining/changes

Examples of metadata in Email documents:

- MS Outlook using MS Word as editor
- Header information reveals author, route, IP address
- Attachments

SHARING A COMPUTER NETWORK

Office sharing offers great opportunities to the solo practitioner or small firm. Such arrangements are permitted by Wisconsin Professional Ethics Opinion E-00-02. Not only can you cut real estate and personnel costs by sharing an office suite and clerical staff, but you have someone else around to bounce ideas off of. And there lies the rub: when you're not really part of a firm, you can't ethically share some of these ideas.

The same is true of sharing office technology resources. In the last few years more and more lawyers have sought to cut costs by making their unused space available to other practitioners, and often the inducements to those practitioners have included shared technology resources such as phone systems and computer networks including fast Internet access. However, just as there can be ethical problems involving confidentiality issues and safekeeping of data with shared office space, there can also be potential problems with shared computer resources.

Do not leave your desktop computer unattended when it is on and you are logged in. Enable the password protection, and set it to override the system when it has been inactive for three minutes or less.

Biometric devices, such as thumbprint readers that authenticate the user may sound a bit geeky today, but with the prices falling to under \$100, expect to see more of this soon.

Log off the network if you are going to be gone longer than an hour.

Use a minimum of eight digit passwords with a combination of numbers and letters—including alternate capitalization of the letters.

Confirm with the law firm network administrator that the network is configured to prevent unauthorized access to your computer. Get this in writing if possible.

There is nothing more important in your office procedures than the regular back-up information stored on your computer. Back up means to copy your important computer files (such as client documents, software applications, time and billing data, and e-mail) onto another computer or media that can be accessed to restore data if your computer crashes, the file is corrupted, or your office is damaged or destroyed.

There are four components to a good back-up system: Automatic back-up software, a large and reliable local storage device, an off-site recipient storage device, and a competent person to make sure it runs correctly. With the growing availability of broadband internet access, online storage for your critical data is also an option. Ranging from the low end with products such as Mozy (www.mozy.com) and Carbonite (www.carbonite.com), to more full featured offerings from Iron Mountain (www.ironmountain.com), Corevault (www.corevault.com), iBackup (www.ibackup.com) and others that provide a wide range of support and services.

Numerous software options are available and often come bundled with the storage device. Forget the old disc and tape devices, and go to external hard drives like Maxtor or ABS. The software is more important than the hardware, because it has to work well for the user or the user won't use it! Too often lawyers buy the back-up device but fail to use it because the software is cumbersome or does not have automatic settings. Consider NTI Backup Now, NovaBACKUP, Retrospect Backup, or full image back-up software such as Norton Ghost (www.symantec.com), Acronis TrueImage (www.acronis.com). To backup just your data files, consider Second Copy (www.secondcopy.com). Whichever method you choose, your office computer should be backed up daily. That is where the competent person comes in! Unless the backup system is used, the technology is worthless. Make sure a competent person carries out this important security step in your firm. Also, do a periodic test to restore a file to make sure your backup system is working.

For one example of a step by step backup plan, see "Don't be an idiot: Backup your data" at the end of Part I.

The current generation of wireless communication gadgets is truly amazing, especially when you compare them with their “bag phone” ancestors of only a decade or so ago. You can sort through your contacts, schedule items on your calendar, read and send email, surf the Internet, read and edit documents, listen to FM radio or pre-recorded music, take and send photos of the funny looking man sleeping on the park bench, and talk to friends and clients, all on the same pocket-sized device.

Wireless communication tools break down into two basic types, based on their feature sets. They are:

Handhelds

Handhelds are the descendants of the personal digital assistant. They typically have an operating system, some pre-installed software, and allow you to download and install other programs, primarily through a cable or cradle, although they may also use an infrared interface, Bluetooth and/or, in the case of wireless handhelds, a connection to a wireless LAN. They are sometimes referred to as “wearable” computers.

Smartphones

Smartphones are the offspring of the marriage of the PDA and the cell phone. They look much like handhelds, but they pack the added punch of allowing you to send and receive calls. Although they may also be capable of synchronizing data with your workstation through a cable, they primarily rely on their wireless connectivity and your cell phone company’s network for information transfer.

In order to understand the current and potential security threats to these tiny life savers, you need to think about their status as “wearable computers” and how they came to be.

The development of the PDA and the convergence of the PDA and the cell phone parallel the development of personal and laptop computers in many ways. Just as computers started out with small operating systems and ran very few simple programs, so did PDAs. The desire for more programs on the PDA encouraged the development of larger and more robust operating systems, which in turn encouraged more robust PDA programs. Finally, owners got tired of having to enter calendar items, contacts and phone numbers into both devices, or having to sync their phones with their PDAs through various means, and the smartphone was born. And along with this convenience came plenty of the same security problems that computer users currently face.

First, because they are small and portable, handhelds and smartphones are infinitely subject to being lost or stolen, placing the information stored on them at risk. If the risk of the information becoming public is great enough, it simply shouldn’t be placed on any device which can be removed from the office in a casual manner. Otherwise, the device should be password protected and, if appropriate, the contents should be encrypted.

Second, these devices are slowly, but surely, becoming subject to all of the ghoulies and ghosties that personal computers encountered when they began to be regularly and consistently connected to the Internet, namely: viruses, worms, and Trojan horses.

In recent history, there have been at least four smartphone infections: Cabir, a “proof of concept” worm that has already gone through A-I versions; Skulls, a Trojan horse which disables cell phone apps, MetalGear.A, a hybrid Trojan horse which disables cell phone anti-virus software and then loads the Cabir worm; and CommWarrior, which sorts through your address book and sends a copy of itself to selected contacts as a multi-media file attached to a text message.

All of these infections targeted smartphones with the Symbian operating system and required the user to download a file. The good news is that Symbian based phones make up only about 2% of the cell phone market currently. While none of them is yet capable of stealing data, they can disable and generally muck up your smartphone and cause you a lot of wasted time and trouble. As the virus writers get better, the possibilities for mischief, such as denial of service attacks and transmission of malicious code through handhelds and cell phones to other networked resources will increase. There is also evidence that cell phone virus writers are starting to work on pests for the Microsoft smartphone operating system. Smartphone security will become a major concern as pointed out in the June 2008 article by John Cox titled “Are smartphone viruses really a threat to your network?” found at www.networkworld.com/news/2008/062308-wireless-questions-1.html?page=1

As their operating systems and features become larger and more complex in order to accommodate consumer needs (or what the cell phone companies tell us we need), every added line of operating system code will become a potential source of additional security problems. And as more lawyers upgrade to more complex cell phone/PDA hybrids, their security worries will only increase.

A couple of current, and slightly more pressing, problems for some cell phone users are “bluejacking” and “bluesnarfing.” These are problems peculiar to Bluetooth® enabled devices.

For the couple of people left in the world who haven’t heard, Bluetooth is a relatively new technology which allows the creation of a PAN (personal area network between two or more connected devices) using radio waves in the 2.4GHz range. Unlike infrared, Bluetooth does not require a clear line of sight and can connect within a standard range of about 30 feet, leaving open the possibility for great convenience in connecting electronic devices quickly and conveniently without wires, as well as the possibility for fun and games – or trouble. Bluejacking fits into the former category, and bluesnarfing into the latter.

Bluejacking is the act of creating a message in the form of a contact with your Bluetooth-enabled phone, and then shooting it to an unsuspecting person within range. As a form of high art, bluejacking messages should usually include a snarky remark about the person’s phone or attire. Then you sit and snicker as the unsuspecting victim looks all around trying to figure out where the message came from, and why. Lawyers are generally pretty thick-skinned, and don’t risk much damage from bluejacking, which doesn’t appear to be illegal unless the communications continue to the point of becoming harassing. If you want to know more about bluejacking, go to www.bluejackq.com, the website of a very precocious British teen who goes by the nom-de-web of jellyellie. Bluesnarfing is another matter.

Bluesnarfing takes place when someone armed with a computer loaded with special software and, often, a directional antenna that can extend the range of Bluetooth, sets up shop in a prime location, waiting for unsuspecting folks to come along and tarry for a while, so that he or she can suck the contents out of the unsuspecting target’s Bluetooth-enabled cell phone, including calendar items, contacts and any multi-media items, such as pictures, associated with them and, in some cases, even the IMEI (International Mobile Equipment Identity) – the phone’s identifying information. Depending on the amount of information in the phone, the process can take as little as thirty seconds or as much as three or four minutes.

The bottom line: How much connectivity do I really need in my practice? Is having a way to capture information while I’m away from the office, and then sync it with my computer when I return a sufficient tradeoff for increased security?

Wireless networking can save a firm the time and expense of running cable to all parts on an office. However, wireless connectivity is neither as reliable nor as fast as wired networks. Yes, it is a close call and getting better, but there are plenty of safety concerns as well.

A wireless router or access point throws a signal about 100 feet, although the signal strength diminishes as it passes through walls. Firms can use this to reach place within the office not previously wired for computers. However, here is where the security concerns come in: Any person with a wireless access card (network card or wireless adaptor) can use your network, and potentially have access to your computer files and documents. The firm must take steps to secure the wireless network from prying eyes. Manufacturers build this security into all routers and access points, but the user must enable it. Whether the security protocol is WEP, WPA, or MAC addresses, make sure you secure the network against intruders.

One final point about wireless office network security: You may find that despite all the best advice and intentions, the network settings and security create too many conflicts and issues. The network may just be too unreliable. In the end, it may be more cost-effective just to run cable and be done with it.

Be sure to secure your home office wireless network too. While not as likely a target, there still may be neighbors who may hijack your network. Many lawyers who successfully install a wireless network are frustrated with security matters. New utilities are just coming to market that makes securing a wireless network a much less frustrating process.

If you are going to use a wireless network, you need to consider the following (there is debate on some of the efficacy of these steps, and while some of them may have varying degrees of effectiveness, they may still be worthwhile to institute):

Enable ENCRYPTION available for wireless networks. Ideally, you want to use Wi-Fi Protected Access 2 (“WPA2”):

Rename the Service Set Identifier (“SSID”): Every wireless Router/Access Point has an SSID which is set at a factory default when initially setup. This is what differentiates one wireless network from another and is sent in plain text. To make it more difficult for someone to identify your wireless network you need to change the standard SSID and Administrator Password of your Router/Access Point. Use something other than your name, a business name or your address.

Disable SSID broadcast if possible: By default, your wireless Router/Access Point broadcasts an identifier so it is readily identifiable. While disabling it doesn’t completely prevent your wireless Router/Access Point from still transmitting this information in certain forms, it will make it undetectable to the average person looking for an easy target.

Limit Number of Computers: If you only have x number of computers which will attach to the wireless network, you should limit the number of machines that can access the network to that number. As long as those computers are connected to the wireless network, no other machines can attach.

Router/Access Point Placement: Since the Router/Access Point generally broadcasts in all directions. Place the access point in the center of your building/office/home if possible - the closer to an outside wall that you place it, the further the range that someone can pick-up a signal. While a true “bad guy” will have a larger antenna to pick up signals, this helps to decrease the likelihood that your neighbor will be able to access your wireless network.

Select infrastructure mode: You can select from 2 wireless modes – ad hoc and infrastructure. ad hoc mode allows wireless equipped computers to communicate directly with each other without the need of first communicating with a Router/Access Point. infrastructure mode requires each wireless equipped computer to use of the Router/Access Point to communicate.

Limit access by specific Media Access Control (“MAC”) address: Each network card is identified by a unique MAC address. By limiting access to the wireless network by MAC address, even if one computer isn’t attached, no one else can communicate with the Router/Access Point since their MAC Address will not be approved for access. This is another one of the suggestions that has its proponents and opponents, but it does add one additional item that someone must obtain to gain access to your wireless network.

Consider disabling DHCP and assigning static IP addresses: This allows you to control which network addresses are assigned and which ones will be recognized by your Router/Access Point. However, this does make it more difficult for you to add other computers and requires a higher level of technical knowledge than many folks have.

MOBILE SECURITY

Many firms are now using notebook computers as full-time replacements for desktops PCs. Lawyers can take them to and from court, depositions, home, etc. Other lawyers are using smartphones or PDAs to store data while on the road. However, this mobility also increases security risks.

Portable devices have a bad habit of being lost, stolen or misplaced. The loss of the computing device is bad enough, but the loss of client data is far worse. All firms must take steps to prevent unauthorized access to client data. All devices must be password protected. Furthermore, if the inadvertent disclosure of client data on your computer would be harmful or embarrassing, then be sure to use encryption technology for all client documents and data.

Mobile security issues also include remote access to your office network from authorized users. The number of lawyers and staff who choose to work outside the office has exploded! We now want to work when we want to work, from home, beach houses, and vacation destinations around the world. The technological tools are many; each firm must to choose the remote tools that work best for their circumstances. However, with such flexibility comes a variety of security issues.

Remote access can take a variety of favors, but all involve Internet connectivity in one way or another. Many small firms use Internet subscription services like GoToMyPC (www.gotomypc.com) or LogMeIn (www.logmein.com) to access their office computer from any other Internet-connected computer. Others use software such as PC Anywhere to access their office computer from home. Still others use more robust (and expensive) tools such as a Microsoft Terminal Server or a Citrix server. A full discussion of these options is beyond the scope of this paper; security remains our focus.

Whichever remote access tool you use, institute the following policies:

All access must be password protected; all passwords to change every 60-90 days; no partner or employee of the firm may disclose his or her password to anyone. This includes prohibiting any user from using the "Remember me" feature (that automatically completes login names and passwords) on their remote computer. This is especially true for employees who use the family computer at home.

Require all remote users to have the same level of Internet security as the law firm: Any computer seeking to access your network must use firewalls, anti-virus software, anti-spyware, etc.

Review the security policies regularly to make sure system integrity is maintained.

If you do not need frequent remote connectivity, try a USB flash drive instead of a remote access system. A USB Flash Drive memory unit is an easy way to transport and share files. This tiny device is smaller than a marking pen yet can hold up to 16 GB or more of information such as client documents, presentations, photos, or music. Just plug and play into the USB port on any computer! It is the perfect tool for transporting files between home and office. Try the Lexar USB JumpDrive Traveler—a flashdrive with extra software so that you can use a public computer and not leave a trace of information behind. For example, if you need to check email and edit a document during your vacation in Disney World, just plug in your JumpDrive Traveler and all your emails and document tracks are saved to the flashdrive, not the host computer. So you can carry documents and work on them confidentially without lugging a computer with you. However, just as with your office computers and notebook computers, you need to insure that any confidential information is protected in the event of loss of theft of a USB drive. Use drive encryption software such as Truecrypt (www.truecrypt.com) or e-Capsule Private Safe (www.eisst.com).

If you are going to use mobile computing then follow these recommendations:

Use a Software Firewall.

Consider using encryption for your e-mail and digital signatures.

Disable your wireless cards ad-hoc option.

Disable file and printer sharing.

Disable your wireless card if you're not working online.

Be aware of anyone looking "over your shoulder" as you enter your passwords.

Consider using VPN software and a VPN endpoint if you have them.

Don't provide your credit card number unless the site is protected by Secure Socket Layer (SSL). These sites are identified by `https://` in their URL.

Discarding or donating an old law office computer is a task that should not be taken lightly. Without properly discarding the information contained on the hard-drive, you may violate your jurisdiction's confidentiality rule. Just deleting everything on the hard drive probably is not enough, as the information can be easily restored and viewed. You should take reasonable additional steps to make sure the information remains confidential.

In most instances, the best thing to do is to reformat the hard drive or use a software utility that "wipes" the hard drive clean. There are numerous products such as Dirk's Boot and Nuke (DBAN) (www.dban.org), WipeDrive and Sure Delete that are shareware programs (available on znet.com) and commercial products such as Norton CleanSweep. But not all drive erasers are the same. Those that claim they meet Department of Defense standards are probably the best place to start.

If the information on your hard drive is VERY sensitive, then consider removing the hard drive from the computer and keeping it or physically destroying it. Yes, it significantly reduces the value of your donation, but isn't it better to be safe than sorry?

Once you've got your old computer wiped clean of any data from your practice, you may need some help finding a new home for it. There could be many groups in your area, from schools to charities, that would love to have your used computer. If not, you will want to take a look at the National Cristina Foundation (www.cristina.org).

The National Cristina Foundation's mission is to provide computer technology to give people with disabilities, students at risk and economically disadvantaged persons the opportunity, through training, to lead more independent and productive lives. The foundation has partner organizations in all fifty states which will match your equipment to individuals or groups who need it. And they'll even tell you what it's worth for purposes of your tax deduction.

The foundation's requirements for accepting a PC are that it have a Pentium class or higher CPU; it must have a hard drive, monitor, keyboard and mouse; and you must include your software license agreements for all software loaded on the machine. Partial systems and systems needing repairs will be considered on a case by case basis.

But if you are like most lawyers, and have squeezed every drop of useful life from your computer equipment, don't despair. There are still some options for getting rid of your dinosaur equipment without hurting the environment. Most of the major computer vendors run their own recycling programs. Gateway (<http://gateway.eztradein.com>), Hewlett-Packard (www.hp.com/recycle), and Dell (www.dell.com/recycle) will take any old computer you want to send them and HP and Dell also participate in the National Cristina Foundation program. If your computer is not suitable for the program, they'll send it to a facility which will break it down into its re-usable components and safely dispose of the rest.

All you have to do is go to the website and fill out the recycling form, pay a processing fee (generally between \$15 and \$35) and pack the equipment up. They'll send someone by a few days later to take it off your hands. What could be easier?

According to the 2007 *ABA Legal Technology Survey Report* 57% of respondents had never received an electronic discovery request and 26% had never made an electronic discovery request. The amendments to the Federal Rules of Civil Procedure (<http://www.uscourts.gov/rules/index.html>) specifically address e-discovery, became effective on December 1, 2006. If you have not been participating in electronic discovery you may find yourself playing catch-up. The pending rules address some of the stickier elements of e-discovery: time and money spent on the process, safe harbor, format, privilege/work product, and subpoenas among other issues. Even now, overlooking, ignoring, or discounting electronic information in the discovery process can lead to sanctions as in the cases of *Zubulake* and *Metropolitan Opera*. Failing to understand the e-discovery process could be considered risking ethical violation for not performing duties with diligence and competence.

The pervasive wisdom suggests that over 90% of all information is created, stored, and accessed electronically. Production of written, printed information only hits the tip of the iceberg. When producing or requesting electronic data you will need to be clear on what format needs to be produced – native format or print. Whereas metadata can be a detriment when inadvertently disclosed, the metadata gathered from discovery of native format documents can deliver the “smoking gun”. Lawyers need to be proactive in the e-discovery approach. Hire an expert, create a strategy, and test it on smaller cases in order to be prepared for the larger cases with terabytes of information. Understand your limitations and allow experts to open and manipulate native files to avoid spoliation. Retaining e-discovery technical experts will allow you to practice law, but you will need to understand the concepts of electronic discovery and embrace it to provide zealous representation for your clients.

Both print and digital resources for legal research have advantages and disadvantages. Print materials must be updated to be accurate, forcing the attorney to seek out updates, replacement volumes, and pocket parts. Online resources, however, while more up-to-date, may encourage a certain amount of complacency – a simple search yields no documents so ergo there must be no applicable law. Good legal research skills come with training and practice. A good researcher will know when to seek a print source or an electronic one. Some electronic resources are easier and more up-to-date than their print counterpart, such as Shepards™. Some resources, such as secondary treatments, are more practical in print.

The Internet offers a tremendous amount of free research resources for law and business. However, make sure that you know the source and authority before using materials. Blogs and wikis proliferate in the legal world and can be great sources of information. However, there is no editorial process so double check and verify anything you find on the free Internet.

Recently *Office Watch* reported that 60 Gmail users lost all of their email because of a program glitch. The article then provides some useful instruction on how to backup web-based email to your local hard drive or server. Ironically, if you are not adequately backing up your hard drive or server, it is likely that the online webmail repository will serve as a backup, if the need arises. The *New York Times* in the recent past published an article by David Pogue entitled "Fewer Excuses for Not Doing a PC Backup". The article describes different online services that offer free and low cost online storage and backup services. While many are lured by the price tag, attorneys must give thought to the potential repercussions of relying on free technology for mission-critical functions.

Free software often provides little to no technical support, or maintenance. Some free software, like Google Desktop Search, can create privacy concerns, depending on its configuration. Free online services in BETA often become fee-based if successful, or lose funding and disappear entirely. Lawyers should be extremely zealous in investigating free downloads and read the EULA (end user license agreement) or Terms of Use to make sure they are not agreeing to download adware or spyware along with the free software, and also check for potential privacy concerns.

As for online backup, while the services mentioned in the *New York Times* article may be useful, online backup providers should be well scrutinized by any law firm considering this backup strategy. The article points out some of the disadvantages, including the time for the initial backup and any restores, security, and corporate longevity. For lawyers add to that the complexities of storing confidential client information with a third party and the repercussions. This is not to say that online backup is inherently too risky for attorneys. It simply means that free and low cost options may not be the right solution.

Companies from LexisNexis to LiveVault/Iron Mountain to eVault are providing secure, fee-based online backup with monitoring. But, even with these companies firms must ensure that the right questions are asked and answered to make a reasonable attempt to protect the firm's data. Courtney Kennaday, SC Bar Practice Management Advisor, has posted a helpful list of questions to ask of online backup providers (<http://www.scbare.org/pmap/>). This list can also help remind firms of questions to ask of *any* free software or online service. The next generation of software is going to be on the Internet - call it .Net, ASP, or SaaS (software as a service) - with some distinct advantages. Lawyers need to be ready to take advantage of this model, and be smart about selecting software and services, whether free or fee. When it comes to business applications and backup the price of free could be high indeed.

DON'T BE AN IDIOT: BACKUP YOUR DATA.

October 25, 2007 Nerino Petro's Compujurist Blog www.compujurist.com

Programming today is a race between software engineers striving to build bigger and better idiot-proof programs, and the Universe trying to produce bigger and better idiots. So far, the Universe is winning.

-Rick Cook, The Wizardry Compiled

I think this quote is very apropos today: as important as backing up your critical data is, I'm still amazed at the number of lawyers that fail to take any steps to protect their data. I last wrote about data backup in Compujurist in 2005 and think it is time to revisit this issue as it continues to be a topic of discussion on e-lists around the country.

There are a wide variety of backup methodologies and schedules from the extremely simple to the incredibly complex. The sample that I set below is just one suggestion and is by no means the only way to create a backup methodology and schedule. The sample plan below is intended for single computers, computers that are in a peer-to-peer environment or are using strictly Windows XP for networking including operating the server. True networks can use a modification of this plan, but it would require different software. However, this sample backup plan provides a reasonable balance between rotating backup media, preparing for a catastrophic loss that does not destroy your office as well as securing your absolutely critical data offsite. I've also tried to take into consideration the complexity, cost and time involved in preparing this sample backup plan.

While it seems that there are as many backup recommendations as there are individuals, I take the view that you should be able restore your entire system meaning not just your data, but all of the programs and software in the event disaster strikes. Many people take the position that they have the backup disks and can simply just reload from those and therefore, there is no need to back up the operating system and all of your programs. While this may be true, think of how much time it will take you to locate all of the disks for each of your programs, install them on your computer, download and install all of your program updates; if you're lucky, you're only talking a matter of hours, but it could be several days. And while your computer system or systems are down, much of your practice will be at a standstill. While I suggested backup plan may leave a small gap between complete backups, it is much easier to download and install updates for a one-week period than it is if you've never made a backup of your entire hard drive at all.

Taking into consideration the points I make above, this generally results in a three-tiered backup approach that includes A) an image of your entire hard drive; B) backups of the data that has changed since the last full backup; and C) online backup of only your data and critical files.

I suggest the following:

1. Purchase a copy of [Acronis True Image 11](#) home for each computer. Ideally, if you have more than one computer, all data is centralized on one of them as it makes backing up much easier. You will also need a minimum of 2 external hard drives (3 is better). You can usually find the hard drives on sale at Best Buy or similar stores every weekend for around \$130 for 250 to 300 Gigabyte Drives (or larger) and you can check there for the software also. If using full-size external hard drives, I recommend that you stick with similar hard drives as you will be able to keep one power adapter at the office and one at home; usually come each manufacturer provides a different power supply for their full-size external hard drives. Another option would be to use a smaller notebook sized external hard drives which generally only require a USB cable to provide their power. The downside to the smaller external drives is the capacity and their speed which will result in a longer backup duration.

2. Install the Acronis True Image software on your computer and make a complete image of your hard drive using the wizard found in the software to one of the external drives. If you have multiple computers, you'll want to make a backup of each and save it to an external drive. This is where the third external hard drive can come in handy as you can back up all of your images to that drive. I also recommend you burn this initial image to a DVD or, if you don't have a writable DVD, then to CD-ROM. Place the disks in a fireproof and secure location. In the event of a

disaster, at a minimum, you can restore back to this original complete disk image. Then on a regular basis, such as quarterly or even after you install new programs, create a new complete image so that you can always back up to that point without having to reinstall all of your programs, operating system and data.

3. On Monday and Wednesday, run a differential backup with a full backup once again on Friday. I recommend a differential, rather than an incremental, backup as a differential back-up backs up all information from the time of the last full back-up through the date of the differential backup; while an incremental backup only backs up the information from the last incremental backup not the last full backup. What this means is the difference between requiring the last full backup and one (the most recent) differential backup to restore your data versus your last full backup and every incremental backup since that full backup to restore your data. For simplicity, I would swap external hard drives out after you make the complete backup on Friday and take the drive with the most current information home with you.

4. Sign up for a free [Mozy](#) online backup account (Mozy has been acquired by [EMC](#) a major player in computer backup systems which offers stability and backing from a solid company). There are numerous other online backup services, but Mozy is simple and provides a free account or a paid unlimited storage account. Mozy will not back up system or program files, and due to the bandwidth limitations, even just backing up your critical data files will take some time. Schedule this to backup only your data files on Tuesdays, Thursdays and Saturdays over the Internet. When you set up your free, 2 GB account (which should be enough to get you started), I also recommend that you use your own encryption password as this will prevent anyone at Mozy or anyone else for that matter, from looking at your data.

IMPORTANT NOTE: YOU MUST MAINTAIN YOUR PASSWORD AS IF YOU LOSE IT, MOZY WILL BE UNABLE TO PROVIDE YOU WITH YOUR PASSWORD SINCE IT IS YOURS AND YOURS ALONE. IF YOU'RE UNCOMFORTABLE WITH THIS, YOU MAY USE THEIR ENCRYPTION, BUT YOU DO RUN THE RISK OF INFORMATION BEING TURNED OVER PURSUANT TO A SUBPOENA OR OTHER ACTION AS SET OUT IN THEIR PRIVACY POLICY.

5. Finally, perform a sample or test restore to ensure that your data is actually being backed up. Murphy's Law of backups provides that your backup will fail when you need it most. One method of doing this is to select several critical files and data types such as your time and billing data and word processing files, renaming several of these files and then doing test restores from the backup data stored on the external hard drive as well as from the online backup service and see if the files will open and if the data appears to be current and correct. Initially, you want to test this with the first backup and then at least biweekly for the first two months. Thereafter, I would recommend doing a test restore at least monthly.

If you add a third external hard drive to this plan, it would become the primary backup for a monthly full backup and then on successive months, each of the hard drives would be rotated through so that at any one time you have a monthly full backup and a weekly full back. This translates into the greatest period of time that you could potentially lose data for would be one week or in the worst case scenario, one month. However, with the online backup of critical data, your data should always be within one or two days of being up-to-date at all times.

For offices using true network operating systems such as Microsoft Server or Microsoft Small Business Server, Acronis makes a product suitable for use on these servers and this procedure can be adapted using such a product. In this event, I would also strongly suggest that each workstation also have a copy of Acronis True Image software installed on it with regular images being made of these systems on a quarterly or semiannual basis or at least when major software is upgraded. You can also use a more traditional backup product such as [EMC Retrospect](#) (server version) which still allows for disaster recovery as well as including the ability to backup connected workstation computers that are connected to the network.

You must weigh your own needs against the potential risks of different backup intervals and what the backup to come up with your own backup plan. However, you need to do some type of backup, even if that's just a backup of your critical data: you can always reinstall your software, but you can't replace your data.